

(19) 世界知的所有権機関
国際事務局



(43) 国際公開日
2004 年10 月14 日 (14.10.2004)

PCT

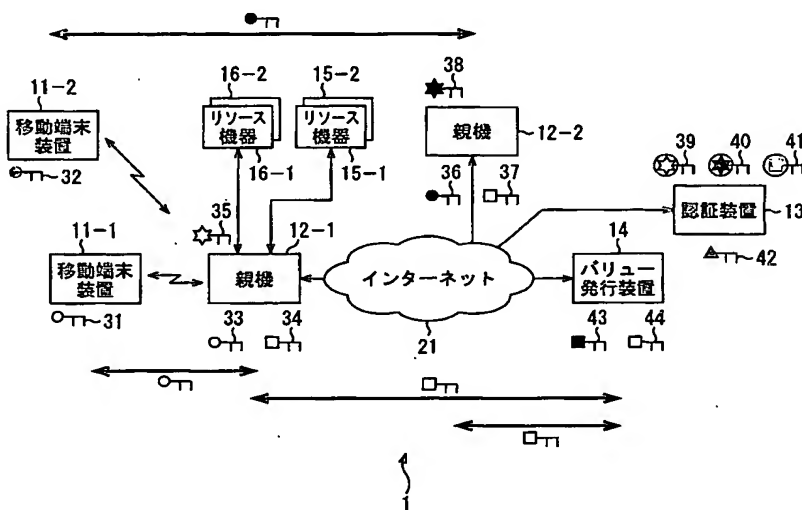
(10) 国際公開番号
WO 2004/088557 A1

- (51) 国際特許分類⁷: G06F 17/60 (72) 発明者; および
(21) 国際出願番号: PCT/JP2004/004338 (75) 発明者/出願人 (米国についてのみ): 板橋 達夫 (ITABASHI, Tatsuo) [JP/JP]; 〒1410001 東京都品川区北品川 6 丁目 7 番 3 5 号 ソニー株式会社内 Tokyo (JP).
(22) 国際出願日: 2004 年3 月26 日 (26.03.2004) (74) 代理人: 稲本 義雄 (INAMOTO, Yoshio); 〒1600023 東京都新宿区西新宿 7 丁目 1 1 番 1 8 号 7 1 1 ビルディング 4 階 Tokyo (JP).
(25) 国際出願の言語: 日本語 (81) 指定国 (表示のない限り、全ての種類の国内保護が可能): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG,
(26) 国際公開の言語: 日本語
(30) 優先権データ: 特願2003-092647 2003 年3 月28 日 (28.03.2003) JP
(71) 出願人 (米国を除く全ての指定国について): ソニー株式会社 (SONY CORPORATION) [JP/JP]; 〒1410001 東京都品川区北品川 6 丁目 7 番 3 5 号 Tokyo (JP).

[続葉有]

(54) Title: INFORMATION PROCESSING SYSTEM, INFORMATION PROCESSING DEVICE, METHOD, AND PROGRAM

(54) 発明の名称: 情報処理システム、情報処理装置および方法、並びにプログラム



- 11-2... MOBILE TERMINAL DEVICE
16-2... RESOURCE DEVICE
15-2... RESOURCE DEVICE
12-2... PARENT DEVICE
11-1... MOBILE TERMINAL DEVICE
12-1... PARENT DEVICE
21... INTERNET
14... VALUE ISSUING DEVICE
13... AUTHENTICATION DEVICE

(57) Abstract: An information processing system, an information processing device, method, and program for a moving user to operate a device in a moved space anonymously. A mobile terminal device (11-2) requests a parent device (12-2) for a resource of a resource device (15). The parent device (12-2) requests a parent device (12-1) for resource permission and the parent device (12-1) notifies consideration required for permitting the resource to the parent device (12-2). The parent device (12-2) requests a value issuing device (14) to transfer the consideration. The value issuing device (14) transfers the consideration of the parent device (12-2) to the parent device (12-1) and transmits a transfer notification to the parent device (12-1). The parent device (12-1) receives the transfer notification and gives the right to use the resource via the parent device (12-2) to the mobile terminal device (11-2). The present invention can be applied to a radio communication system.

[続葉有]



SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ,
VC, VN, YU, ZA, ZM, ZW.

NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG,
CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

- (84) 指定国 (表示のない限り、全ての種類の広域保護が可能): ARIPO (BW, GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), ヨーロッパ (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC,

添付公開書類:

— 国際調査報告書

2文字コード及び他の略語については、定期発行される各PCTガゼットの巻頭に掲載されている「コードと略語のガイダンスノート」を参照。

(57) 要約: 本発明は、ユーザが移動する場合においても、移動した空間にある機器を、匿名のまま操作することができるようにする情報処理システム、情報処理装置および方法、並びにプログラムに関する。移動端末装置 11-2 は、親機 12-2 にリソース機器 15 のリソースを要求する。親機 12-2 は、親機 12-1 にリソース許可を要求し、親機 12-1 は、親機 12-2 に対してリソースを許可するために必要な対価を通知する。親機 12-2 は、バリュー発行装置 14 に対価の移動を要求する。バリュー発行装置 14 は、親機 12-2 の対価を親機 12-1 に移動し、振込み通知書を親機 12-1 に送信する。親機 12-1 は、その振込み通知書を受信し、リソース利用の権利を親機 12-2 を経由して移動端末装置 12-2 に与える。本発明は、無線通信システムに適用することができる。

明細書

情報処理システム、情報処理装置および方法、並びにプログラム

技術分野

- 5 本発明は、情報処理システム、情報処理装置および方法、並びにプログラムに関し、特に、ユーザが移動する場合においても、移動した空間にある機器を、匿名のままユーザの嗜好に合わせた操作性で操作させることができるようにした情報処理システム、情報処理装置および方法、並びにプログラムに関する。

10 背景技術

近年、携帯型のパーソナルコンピュータ、携帯電話などが普及し、多くのユーザがこれら通信機能、情報処理機能を有する小型の装置を携帯し、屋外で、あるいは移動先においてネットワークに接続してネットワークを介する通信を行なっている。

- 15 ここで、既存のインフラを利用したシステムとして、すでに存在する様々な通信網を適宜切り替えて利用するパーソナル通信サービス分散システムが提案されている（例えば、特開平 8－5 6 2 6 3 号公報）。このシステムは、例えば電子メールサービスや電話サービス等の異なるネットワーク通信網を統合して利用することを可能としたシステムである。

- 20 しかしながら、このようなシステムにおいて、ユーザが外出中のような状況で、ユーザにメッセージを伝達することはできても、出先に有るたまたま身近な機器を、自らの所有する同種機種と同じ感覚で利用するなど、周囲に置いてある機器を自分に合わせた使い方をすることはできず、結局ユーザは、使い慣れた端末（例えば、PC など）を持ち運ばなくてはならなかった。

- 25 このような問題に対して、自宅のホームサーバに自分の嗜好等の情報を持ち、その情報を基に出先の機器の振る舞いを変化させるシステムを、本出願人が先に、特願 2 0 0 3－2 9 2 5 8 7 号で提案している。

しかしながら、この方法では、一方的に他者のリソースを使い続けるユーザや、他者のリソースを使う機会が少ないにもかかわらず、自ら所有するリソースを提供し続けるユーザがいる場合、需給のバランスがとれなくなる恐れがある。

そこで、ユーザが、他者の所有するリソースを利用するために必要な対価を、

5 自分と他者の対価を管理する装置を介して支払うシステムが必要となる。

このためには、例えばクレジットカード番号をやり取りすることによりリソースの提供者とリソースのユーザ側との間で対価をやり取りする方法が考えられる。

しかしながら、クレジットカード番号はプライバシー情報のため、他者に知られるには抵抗があり、また、クレジットカードを利用するためには自分の個人情報
10 報をカード会社に登録しなければならず、つまりユーザの個人情報は対価を管理する装置に管理される。従って、ユーザが対価を管理する装置に対しても匿名のまま対価を支払い、他者の所有するリソースを利用することは困難であった。

このため、対価を前提に公共の場で通信サービスを行っている無線 LAN

(Local Area Network) 等の事業者とのシームレスなサービスをユーザに提供
15 することは困難であった。

発明の開示

本発明は、このような状況に鑑みてなされたものであり、ユーザが移動する場合においても、移動した空間にある機器を、自分の慣れ親しんだ操作方法で操作
20 できるなど、自分の嗜好などの個人の情報を基に機器の動作を変化させ、かつ匿名のままその対価を支払うことができるようにするものである。

本発明の情報処理システムは、ユーザにより操作される端末と、リソースを提供する第 1 の親機と、ユーザの個人情報を記憶する第 2 の親機と、電子バリューを管理するバリュー装置とを備える情報処理システムであって、端末は、第 1 の
25 親機が提供するリソースを要求する信号を、第 2 の親機に送信するリソース要求信号送信手段と、第 1 の親機が提供するリソースを利用する利用権を、第 2 の親機から取得する第 1 の利用権取得手段とを有し、利用権を、第 1 の親機に提示し

て、第1の親機が提供するリソースを利用し、第1の親機は、リソースの提供に対する対価としての電子バリューが、第2の親機から第1の親機に振り込まれたことの振込み通知を、バリュー装置から受信する振込み通知受信手段と、振込み通知に応じて、第2の親機に対して、利用権を発行する利用権発行手段とを有し、
5 端末が、利用権を提示した場合に、自身が有するリソースの利用を許可し、第2の親機は、端末装置から送信されてくる、リソースを要求する信号に応じて、第1の親機への電子バリューの振込みを、バリュー装置に要求する電子バリュー振込み要求手段と、電子バリューの振込みに応じて、第1の親機が発行する利用権を取得する第2の利用権取得手段と、第2の利用権取得手段において取得された
10 利用権を、端末に提供する利用権提供手段とを有し、バリュー装置は、第2の親機からの要求に応じて、第1の親機に電子バリューを振り込む電子バリュー振込み手段と、第1の親機への電子バリューの振込み通知を、第1の親機に送信する振込み通知送信手段とを有することを特徴とする。

本発明の第1の情報処理装置は、リソースを提供する第1の親機が提供するリ
15 ソースを要求する信号を、ユーザの個人情報を記憶する第2の親機に送信するリソース要求信号送信手段と、第1の親機が提供するリソースを利用する利用権を、第2の親機から取得する利用権取得手段とを備え、利用権を、第1の親機に提示して、第1の親機が提供するリソースを利用することを特徴とする。

第2の親機との間で、ユーザが第2の親機が記憶している個人情報に対応する
20 正当なユーザであることの認証を行う認証手段をさらに備えるようにすることができる。

リソース要求信号送信手段と利用権取得手段は、第1の親機を介して、第2の親機とやりとりするようにすることができる。

リソース要求信号送信手段と利用権取得手段は、第2の親機との間で、データ
25 を暗号化してやりとりするようにすることができる。

リソースは、装置、情報、または情報に対するライセンスであるようにすることができる。

本発明の第 1 の情報処理装置の情報処理方法は、リソースを提供する第 1 の親機が提供するリソースを要求する信号を、ユーザの個人情報を記憶する第 2 の親機に送信するリソース要求信号送信ステップと、第 1 の親機が提供するリソースを利用する利用権を、第 2 の親機から取得する利用権取得ステップとを含み、利用権を、第 1 の親機に提示して、第 1 の親機が提供するリソースを利用することを特徴とする。

本発明の第 1 の情報処理装置のプログラムは、リソースを提供する第 1 の親機が提供するリソースを要求する信号を、ユーザの個人情報を記憶する第 2 の親機に送信するリソース要求信号送信ステップと、第 1 の親機が提供するリソースを利用する利用権を、第 2 の親機から取得する利用権取得ステップとを含み、利用権を、第 1 の親機に提示して、第 1 の親機が提供するリソースを利用することを特徴とする。

本発明の第 2 の情報処理装置は、リソースの提供に対する対価としての電子バリューが、ユーザの個人情報を記憶する親機から振り込まれたことの振込み通知を、電子バリューを管理するバリュー装置から受信する振込み通知受信手段と、振込み通知に応じて、親機に対して、自身が有するリソースを利用する利用権を発行する利用権発行手段とを備え、端末が、親機から取得した利用権を提示した場合に、自身が有するリソースの利用を許可することを特徴とする。

バリュー装置との間で、電子バリューを扱う正当な装置であることの認証を行う認証手段をさらに備えるようにすることができる。

振込み通知が正当であることの認証を行う認証手段をさらに備えるようにすることができる。

リソースは、装置、情報、または情報に対するライセンスであるようにすることができる。

本発明の第 2 の情報処理装置の情報処理方法は、リソースの提供に対する対価としての電子バリューが、ユーザの個人情報を記憶する親機から振り込まれたことの振込み通知を、電子バリューを管理するバリュー装置から受信する振込み通

知受信ステップと、振込み通知に応じて、親機に対して、自身が有するリソースを利用する利用権を発行する利用権発行ステップとを含み、端末が、親機から取得した利用権を提示した場合に、自身が有するリソースの利用を許可することを特徴とする。

- 5 本発明の第2の情報処理装置のプログラムは、リソースの提供に対する対価としての電子バリューが、ユーザの個人情報を記憶する親機から振り込まれたことの振込み通知を、電子バリューを管理するバリュー装置から受信する振込み通知受信ステップと、振込み通知に応じて、親機に対して、自身が有するリソースを利用する利用権を発行する利用権発行ステップとを含み、端末が、親機から取得
- 10 した利用権を提示した場合に、自身が有するリソースの利用を許可することを特徴とする。

- 本発明の第3の情報処理装置は、端末からの要求に応じて、端末にリソースを提供する親機への、リソースの提供に対する対価としての電子バリューの振込みを、電子バリューを管理するバリュー装置に要求する電子バリュー振込み要求手段と、電子バリューの振込みに応じて、親機が発行する、その親機が有するリ
- 15 ースを利用する利用権を取得する利用権取得手段と、利用権取得手段において取得された利用権を、端末に提供する利用権提供手段とを備えることを特徴とする。

バリュー装置との間で、電子バリューを扱う正当な装置であることの認証を行う認証手段をさらに備えるようにすることができる。

- 20 端末との間で、ユーザが個人情報に対応する正当なユーザであることの認証を行う認証手段をさらに備えるようにすることができる。

リソースは、装置、情報、または情報に対するライセンスであるようにすることができる。

- 本発明の第3の情報処理装置の情報処理方法は、端末からの要求に応じて、端
- 25 末にリソースを提供する親機への、リソースの提供に対する対価としての電子バリューの振込みを、電子バリューを管理するバリュー装置に要求する電子バリュー振込み要求ステップと、電子バリューの振込みに応じて、親機が発行する、そ

の親機が有するリソースを利用する利用権を取得する利用権取得ステップと、利用権取得ステップの処理において取得された利用権を、端末に提供する利用権提供ステップとを含むことを特徴とする。

本発明の第 3 の情報処理装置のプログラムは、端末からの要求に応じて、端末
5 にリソースを提供する親機への、リソースの提供に対する対価としての電子バリューの振込みを、電子バリューを管理するバリュー装置に要求する電子バリュー振込み要求ステップと、電子バリューの振込みに応じて、親機が発行する、その親機が有するリソースを利用する利用権を取得する利用権取得ステップと、利用権取得ステップの処理において取得された利用権を、端末に提供する利用権提供
10 ステップとを含むことを特徴とする。

本発明の第 4 の情報処理装置は、ユーザにより操作される端末にリソースを提供する第 1 の親機に対する、そのリソースの提供に対する対価としての電子バリューの振込みを、ユーザの個人情報を記憶する第 2 の親機からの要求に応じて行う電子バリュー振込み手段と、第 2 の親機から第 1 の親機への電子バリューの振
15 込みが行われたことを表す振込み通知を、第 1 の親機に送信する振込み通知送信手段とを備えることを特徴とする。

第 1 または第 2 の親機との間で、電子バリューを扱う正当な装置であることの認証を行う認証手段をさらに備えるようにすることができる。

第 1 と第 2 の親機の電子バリューを記憶する記憶手段をさらに備え、電子バリュー振込み手段は、記憶手段に記憶された電子バリューを書き換えることにより、
20 第 2 の親機から第 1 の親機に対して、電子バリューを振り込むようにすることができる。

電子バリュー振込み手段は、第 2 の親機から電子バリューを取得し、その電子バリューを第 1 の親機に送信することにより、第 2 の親機から第 1 の親機に対し
25 て、電子バリューを振り込むようにすることができる。

本発明の第 4 の情報処理装置の情報処理方法は、ユーザにより操作される端末にリソースを提供する第 1 の親機に対する、そのリソースの提供に対する対価と

しての電子バリューの振込みを、ユーザの個人情報を記憶する第2の親機からの要求に応じて行う電子バリュー振込みステップと、第2の親機から第1の親機への電子バリューの振込みが行われたことを表す振込み通知を、第1の親機に送信する振込み通知送信ステップとを含むことを特徴とする。

- 5 リソースは、装置、情報、または情報に対するライセンスであるようにすることができる。

本発明の第4の情報処理装置のプログラムは、ユーザにより操作される端末にリソースを提供する第1の親機に対する、そのリソースの提供に対する対価としての電子バリューの振込みを、ユーザの個人情報を記憶する第2の親機からの要求に応じて行う電子バリュー振込みステップと、第2の親機から第1の親機への電子バリューの振込みが行われたことを表す振込み通知を、第1の親機に送信する振込み通知送信ステップとを含むことを特徴とする。

本発明においては、端末により、第1の親機が提供するリソースを要求する信号が、第2の親機に送信され、記第1の親機が提供するリソースを利用する利用
15 権が、第2の親機から取得される。そして、利用権が、第1の親機に提示され、第1の親機が提供するリソースが利用される。また、第1の親機により、リソースの提供に対する対価としての電子バリューが、第2の親機から第1の親機に振り込まれたことの振込み通知が、バリュー装置から受信され、振込み通知に応じて、第2の親機に対して、利用権が発行される。また、第1の親機により、端末
20 により利用権が提示された場合に、自身が有するリソースの利用が許可される。第2の親機により、端末装置から送信されてくる、リソースを要求する信号に応じて、第1の親機への電子バリューの振込みが、バリュー装置に要求され、電子バリューの振込みに応じて、第1の親機が発行する利用権が取得される。また、第2の親機により、取得された利用権が、端末に提供される。バリュー装置によ
25 り、第2の親機からの要求に応じて、第1の親機に電子バリューが振り込まれ、第1の親機への電子バリューの振込み通知が、第1の親機に送信される。

図面の簡単な説明

図 1 は、本発明を適用した通信システムの構成例を示すブロック図である。

図 2 は、図 1 の移動端末装置の構成例を示すブロック図である。

図 3 は、図 2 の移動端末装置におけるリソース取得処理を説明するフローチャートである。

図 4 は、図 3 のステップ S 2 およびステップ S 6 の共通秘密鍵認証処理を説明するフローチャートである。

図 5 は、図 3 のステップ S 5 のリソース情報取得処理を説明するフローチャートである。

10 図 6 は、図 1 の親機の構成例を示す図である。

図 7 は、図 6 のリソース制御部の構成例を示す図である。

図 8 は、図 6 の親機におけるリソース制御処理を説明するフローチャートである。

図 9 は、図 8 のステップ S 7 1 のリソース送信処理を説明するフローチャート
15 である。

図 10 は、図 8 のステップ S 7 1 のリソース送信処理を説明するフローチャートである。

図 11 は、電子証明書例を示す図である。

図 12 は、図 6 の親機におけるリソース情報送信処理を説明する図である。

20 図 13 は、図 6 の親機におけるリソース利用条件文発行処理を説明するフローチャートである。

図 14 は、図 6 の親機における権利文発行要求処理を説明するフローチャートである。

図 15 は、図 1 のバリュー発行装置の構成例を示す図である。

25 図 16 は、図 15 のバリュー発行装置における振込み通知書送信処理を説明するフローチャートである。

図 17 は、図 1 の認証装置の構成例を示す図である。

図 18 は、図 17 の認証装置における電子証明書判定処理を説明する図である。

図 19 は、図 1 の通信システムにおけるリソース取得処理を説明する図である。

図 20 は、他のシステムの構成例を示す図である。

図 21 は、図 20 に示したシステムの動作を説明するフローチャートである。

5

発明を実施するための最良の形態

以下、図を参照し本発明の実施の形態について説明する。

図 1 は、本発明を適用した情報処理システム 1 の構成例を示すブロック図である。

- 10 この情報処理システム 1 では、親機 12 とバリュウ発行装置 14 間の処理を安全確実にを行うために用いられた公開鍵暗号 (PKI (Public Key Infrastructure)) 系の暗号技術を用いてセキュリティを確保する。

図 1 の例においては、2 人のユーザが、それぞれ移動端末装置 11-1 と移動端末装置 11-2 を有している。ユーザは、必ず 1 つの親機にユーザの個人情報

- 15 (利用履歴、嗜好、決済関連等) を格納し、ユーザの認証情報として共通秘密鍵を取得する。この例では、ユーザと親機が共通秘密鍵として同じパスフレーズを有しており、ユーザと親機は、同じパスフレーズを有することを確認することで、ユーザを認証する。

- 20 また、この例では、移動端末装置 11-1 のユーザは親機 12-1 に、移動端末装置 11-2 のユーザは親機 12-2 に、ユーザの個人情報を格納している。

- さらに、移動端末装置 11-1 は、その移動端末装置 11-1 のユーザの個人情報を格納した親機 12-1 と直接無線で通信可能な位置にあり、移動端末装置 11-2 は、その移動端末装置 11-2 のユーザの個人情報を格納した親機 12-2 とは遠隔地に設置された、親機 12-1 と直接無線で通信できる位置にある。
- 25 従って、移動端末装置 11-2 は、親機 12-2 とは無線で通信することが困難であるが、親機 12-1 とは直接無線で通信できる。

移動端末装置 11-1 と移動端末装置 11-2 は、ユーザとともに移動し、無線通信を用いてユーザからの指示に対応する信号を親機 12-1 に送信する。また、移動端末装置 11-1 と移動端末装置 11-2 は、無線通信を用いて、親機 12-1 からの信号を受信する。

- 5 以下、移動端末装置 11-1 と移動端末装置 11-2 のそれぞれを個々に区別する必要がない場合、適宜、まとめて、移動端末装置 11 と称する。

この移動端末装置 11 とユーザとは、依存関係がなく、ユーザが移動端末装置 11 を利用するときのみ、移動端末装置 11 は、ユーザの認証を行う。従って、移動端末装置 11 には、ユーザの認証情報の入力機能が備えられている。

- 10 図 1 の例においては、移動端末装置 11-1 および移動端末装置 11-2 のユーザは、ユーザの認証情報として、共通秘密鍵 31 および共通秘密鍵 32 を、それぞれ入力している。

親機 12-1 は、所定の空間に配置され、無線通信を用いて、移動端末装置 11 から送信された信号を受信するとともに、移動端末装置 11 に信号を送信する。

- 15 また、親機 12-1 は、ユーザに提供する情報であるコンテンツ等のリソースを有するリソース機器 15-1、リソース機器 15-2、リソース機器 16-1、およびリソース機器 16-2 と接続されている。さらに、親機 12-1 は、インターネット 21 を介して、認証装置 13 およびバリュー発行装置 14 と接続されている。

- 20 ここで、親機 12-1 は、例えば、移動端末装置 11-1 のユーザのユーザ宅の、いわゆるホームサーバで構成することができる。同様に、親機 12-2 も、例えば、移動端末装置 11-2 のユーザのユーザ宅のホームサーバで構成することができる。

- 25 以下、リソース機器 15-1 とリソース機器 15-2 のそれぞれを個々に区別する必要がない場合、適宜、まとめて、リソース機器 15 と称する。また、リソース機器 16-1 とリソース機器 16-2 のそれぞれを個々に区別する必要がない場合、適宜、まとめて、リソース機器 16 と称する。

これにより、移動端末装置 1 1 は、親機 1 2 - 1 を介して、親機 1 2 - 1 に接続されたリソース機器 1 5、リソース機器 1 6、およびインターネット 2 1 を介して接続された機器との通信ができる。

5 また、親機 1 2 - 1 は、ユーザの認証情報として共通秘密鍵 3 3 を格納している。即ち、この共通秘密鍵 3 3 は、移動端末装置 1 1 - 1 のユーザに入力された共通秘密鍵 3 1 と等しくなっている。さらに、親機 1 2 - 1 は、バリュウ発行装置 1 4 により送信された共通秘密鍵 3 4 と、自らの正当性を証明する秘密鍵 3 5 を記憶している。

10 親機 1 2 - 2 は、インターネット 2 1 を介して、親機 1 2 - 1、認証装置 1 3、およびバリュウ発行装置 1 4 と接続されている。

また、親機 1 2 - 2 は、ユーザの認証情報として共通秘密鍵 3 6 を格納している。この共通秘密鍵 3 6 は、移動端末装置 1 1 - 2 のユーザに入力された共通秘密鍵 3 2 と等しくなっている。さらに、親機 1 2 - 1 は、バリュウ発行装置 1 4 により送信された共通秘密鍵 3 7 と、自らの正当性を証明する秘密鍵 3 8 を記憶
15 している。

以下、親機 1 2 - 1 と親機 1 2 - 2 のそれぞれを個々に区別する必要がない場合、適宜、まとめて、親機 1 2 と称する。

20 認証装置 1 3 は、親機 1 2 - 1 の秘密鍵 3 5 に対応する公開鍵 3 9、親機 1 2 - 2 の秘密鍵 3 8 に対応する公開鍵 4 0、およびバリュウ発行装置 1 4 の後述する秘密鍵 4 3 に対応する公開鍵 4 1 を記憶する。また、認証装置 1 3 は、自らの正当性を証明する秘密鍵 4 2 を記憶する。

25 認証装置 1 3 は、他の装置からの要求に応じて公開鍵を検索し、その公開鍵を他の装置に送信する。秘密鍵とそれに対応する公開鍵は、一方の鍵に基づいて生成された暗号文を他方の鍵を用いて復号できる関係にある。また、認証装置 1 3 は、電子証明書（図 1 1）の発行および鍵の失効管理を行う。

バリュウ発行装置 1 4 は、親機 1 2 - 1 と親機 1 2 - 2 に対し、バリュウ（電子バリュウ）の発行および流通管理を行う。バリュウ発行装置 1 4 は、自らの正

当性を証明する秘密鍵 4 3 および共通秘密鍵 4 4 を記憶している。バリュー発行装置 1 4 は、共通秘密鍵 4 4 をバリューを発行する相手である親機 1 2 - 1 と親機 1 2 - 2 に送信し、親機 1 2 - 1 に共通秘密鍵 3 4 として記憶させるとともに、親機 1 2 - 2 に共通秘密鍵 3 7 として記憶させる。即ち、共通秘密鍵 3 4、共通
5 秘密鍵 3 7、および共通秘密鍵 4 4 は等しい。

ユーザは、自身の個人情報（利用履歴、嗜好、決済関連情報等）を自身の親機 1 2 - 1、1 2 - 2 にのみ格納し、共通秘密鍵 3 3、3 6 を取得する。そして、この共通秘密鍵を用いて、全ての通信を行うことにより、ユーザは、匿名性を保ち、安全に通信を行うことができる。

10 なお、上述の例では、2 個の移動端末装置が存在するが、移動中のユーザが多数いる場合、その数だけの移動端末装置が存在するものとする。また、上述の例では、2 個の親機が存在するが、各空間には、それぞれの空間に必要な数だけの親機が存在するものとする。

また、共通秘密鍵 3 1 と共通秘密鍵 3 2 は、移動端末装置 1 1 のユーザを認証
15 するための鍵である。共通秘密鍵 3 4、共通秘密鍵 3 7、および共通秘密鍵 4 4 は、バリューを扱う正当な装置であることを認証するための鍵である。秘密鍵 3 5、秘密鍵 3 8、および秘密鍵 4 3 は、自らの正当性を証明するための鍵であり、装置間における通信中の改ざんを防止する。

以上のように構成される通信システム 1 によって、例えば、移動端末装置 1 1
20 - 2 のユーザがその個人情報を記憶していない親機 1 2 - 1 のリソースを利用する場合には、移動端末装置 1 1 - 2 は、親機 1 2 - 1 の利用したいリソースを指定し、個人情報を記憶している親機 1 2 - 2 に、そのリソースの利用を要求する。親機 1 2 - 2 は、移動端末装置 1 1 - 2 からリソースが要求されると、親機 1 2 - 1 に対するリソース利用に必要なバリューの支払いを、バリュー発行装置 1 4
25 に要求する。

バリュー発行装置 1 4 は、親機 1 2 - 2 のバリューを親機 1 2 - 1 に移動させ、親機 1 2 - 1 にバリューの振込みが行われたことを表す振込み通知を発行する。

親機 1 2 - 1 は、バリュー発行装置 1 4 から振り込み通知を受信すると、親機 1 2 - 2 にリソースを利用する利用権を発行する。親機 1 2 - 2 は、親機 1 2 - 1 から利用権が発行されると、その利用権を移動端末装置 1 1 - 2 に送信する。移動端末装置 1 1 - 2 は、その利用権を親機 1 2 - 1 に提示し、リソースを要求する。親機 1 2 - 2 は、移動端末装置 1 1 - 2 から利用権を提示された場合、リソースの利用を許可する。

次に、図 2 は、図 1 の移動端末装置 1 1 の詳細構成例を示している。

図 2 の例では、移動端末装置 1 1 - 1 を説明するが、移動端末装置 1 1 - 2 も同様に構成される。

10 移動端末装置 1 1 - 1 は、CPU (Central Processing Unit) 6 1、ROM (Read Only Memory) 6 2、RAM (Random Access Memory) 6 3、表示部 6 4、リーダライタ 6 5、送信部 6 6、アンテナ 6 7、受信部 6 8、暗号/復号部 6 9、および操作入力部 7 0 から構成される。

15 なお、移動端末装置 1 1 - 1 のユーザは、あらかじめ取得した共通秘密鍵 3 1、自身の親機 1 2 - 1 が接続しているリソースの情報、および自身の親機 1 2 - 1 のネットワーク上のアドレスを格納した非接触 IC (Integrated Circuit) カード 7 1 を有している。

20 このように、共通秘密鍵 3 1 を改ざんが困難な非接触 IC カードに安全に格納することにより、通信システムの安全性と利便性を向上させることができる。また、非接触 IC カードは、非接触のインターフェースであるので、利用時の利便性が向上し、かつ簡単な操作で処理が可能になる。

この非接触 IC カードとしては、例えば、FeliCa (商標) のような対タンパ性の高い IC チップが用いられる。なお、共通秘密鍵 3 1 などは、非接触型ではなく接触型のデバイスに格納することも可能である。但し、便利性及びデバイスの劣化に対する耐性を考えると、接触型ではなく、非接触型を採用するのが望ましい。

CPU 6 1 は、ROM 6 2 に記憶されているプログラムに従って各種の処理を実行する。RAM 6 3 には、CPU 6 1 が各種の処理を実行する上において必要なデータなどが適宜記憶される。

表示部 6 4 は、CPU 6 1 からの指令により、例えば、移動端末装置 1 1 - 1 が
5 利用できるリソースの情報を表示する。リーダライタ 6 5 は、ユーザが有する非接触 I C カード 7 1 に封じ込められた（格納された）共通秘密鍵 3 1、ユーザの個人情報を記憶した親機 1 2 - 1 が接続しているリソースの情報、および個人情報を記憶した親機 1 2 - 1 のネットワーク上のアドレスを読み込み、CPU 6 1 に共通秘密鍵 3 1、リソース情報、およびアドレスを供給する。ここで、また、リー
10 ダライタ 6 5 は、CPU 6 1 からの指令により、必要に応じて非接触 I C カード 7 1 にデータを書き込む。

送信部 6 6 は、CPU 6 1 からの指令により、親機 1 2 - 1 に送信する信号をアンテナ 6 7 に供給する。アンテナ 6 7 は、送信部 6 6 から供給された信号を、無線通信を用いて親機 1 2 - 1 に送信する。さらに、アンテナ 6 7 は、親機 1 2 -
15 1 から送信された信号を受信し、その信号を受信部 6 8 に供給する。受信部 6 8 は、アンテナ 6 7 から供給された信号を、CPU 6 1 に供給する。

暗号/復号部 6 9 は、非接触 I C カード 7 1 から読み込まれた共通秘密鍵 3 1 を暗号化したり、受信部 6 8 で受信した暗号化された共通秘密鍵を復号し、その復号した共通秘密鍵をさらに暗号化する。操作入力部 7 0 は、ユーザにより操作
20 され、その操作に対応する信号が CPU 6 1 に供給される。

図 3 は、図 2 の移動端末装置 1 1 がリソースを取得する処理を説明するフローチャートである。なお、ユーザは、予め個人情報を自身の親機に格納しており、共通秘密鍵 3 1（3 2）、その親機に接続されているリソースの情報、およびその親機のネットワーク上のアドレスは非接触 I C カード 7 1 に記憶されているものとする。図 3 の処理は、例えば、ユーザが操作入力部 7 0 を操作して親機 1 2 -
25 1 に接続されているリソースの取得を要求したときに開始される。

ステップS 1において、CPU 6 1は、移動端末装置 1 1を使用するユーザの個人情報が格納されている自身の親機（以下、適宜、本親機と称する）と無線通信が可能であるかどうかを判定する。例えば、移動端末装置 1 1は、無線通信が可能な機器を検索し、検索された機器の中に本親機が含まれているかどうかを判定する。

ステップS 1で、CPU 6 1は、本親機と無線通信が可能であると判定した場合、ステップS 2に進み、CPU 6 1は、本親機（例えば、移動端末装置 1 1－1の場合、親機 1 2－1）との間で共通秘密鍵認証処理を行ない、ステップS 3に進む。この共通秘密鍵認証処理の詳細は、図 4 で後述する。

10 ステップS 3では、CPU 6 1は、ユーザが操作入力部 7 0を操作することにより指定したリソースを要求する信号を、送信部 6 6を制御して、アンテナ 6 7から本親機である、例えば、親機 1 2－1に送信する。即ち、ユーザは、非接触ICカード 7 1に記憶され、リーダライタ 6 5から読み込まれたリソース情報を表示部 6 4に表示させ、そのリソース情報を見て、取得したいリソースを指定する。

15 これにより、そのリソースを要求する信号がアンテナ 6 7から送信される。なお、以下の説明では、CPU 6 1が送信部 6 6を制御して、信号を送信することを、単に、CPU 6 1が信号を送信するという。

ステップS 3の処理後は、ステップS 4に進み、アンテナ 6 7は、ステップS 3のリソース要求信号に対応して親機 1 2－1から送信されたリソース（を使用

20 するのに必要な情報）を受信し、受信部 6 8を介してCPU 6 1に供給する。そして、CPU 6 1は、そのリソースをRAM 6 3に保持する。なお、以下の説明では、アンテナ 6 7が信号を受信し、受信部 6 8を介して、CPU 6 1にその信号を供給することを、単に、CPU 6 1が信号を受信するという。

一方、ステップS 1で、CPU 6 1は、本親機と無線通信が可能ではないと判定

25 した場合（例えば、移動端末装置 1 1－2が、親機 1 2－2と通信できない場合）、ステップS 5に進み、リソース情報取得処理を行ない、ステップS 6に進む。即ち、例えば、移動端末装置 1 1－2については、現在、その移動端末装置

1 1-2と通信できる親機1 2-1が本親機ではないので、移動端末装置1 1-2は、親機1 2-1が接続しているリソースの情報を非接触ICカード7 1に記憶していない。従って、移動端末装置1 1-2は、親機1 2-1が接続しているリソースの情報を取得する必要がある、このため、ステップS 5において、リソース情報取得処理が行なわれる。このリソース情報取得処理の詳細は、図5で後述する。

ステップS 6において、CPU 6 1は、本親機（親機1 2-2）との間で共通秘密鍵認証処理を行い、ステップS 7に進む。なお、いまの場合、移動端末装置1 1-2は、本親機である親機1 2-2と直接無線通信することはできないため、
10 ステップS 6の共通秘密鍵認証処理は、後述するように、移動端末装置1 1-2と親機1 2-2との間で、親機1 2-1およびインターネット2 1を介した通信を行うことにより実行される。この共通秘密鍵認証処理の詳細は、図4で後述する。

ステップS 7では、CPU 6 1は、非接触ICカード7 1から、親機1 2-2の
15 アドレスを読み出す。そして、ユーザが操作入力部7 0を操作することにより指定したリソースを要求する信号（リソース利用権発行要求）を親機1 2-2のアドレスとともに、親機1 2-1に送信し、インターネット2 1経由で親機1 2-2に送信する。即ち、ユーザは、ステップS 5で取得した親機1 2-1が接続しているリソースのリソース情報を表示部6 4に表示させ、そのリソース情報を見て、取得したいリソースを指定する。これにより、そのリソースを利用する権利
20 を要求する信号として、リソース利用権発行要求が、移動端末装置1 1-2から、親機1 2-1およびインターネット2 1を介して、本親機である親機1 2-2に送信される。

ここで、移動端末装置1 1-2は、上述のように、親機1 2-2のアドレスを
25 親機1 2-1に知らせる。これにより、移動端末装置1 1-2は、無線通信可能な親機1 2-1とインターネット2 1を介して、本親機である親機1 2-2と通信が可能になる。

ステップS 7の処理後は、ステップS 8に進み、CPU 6 1は、親機1 2-1から、リソースを取得する権利を記載した権利文のデータであるリソース利用権を受信したか否かを判定する。ステップS 8で、CPU 6 1は、親機1 2-1から権利文を受信したと判定した場合、移動端末装置1 1-2は、親機1 2-1に接続しているリソースを利用する権利があるので、ステップS 9に進み、親機1 2-1に、受信した権利文とリソース要求信号を送信する。ステップS 9の処理後は、ステップS 10に進み、CPU 6 1は、リソース要求信号に対応して、親機1 2-1から送信されたリソース（を利用するのに必要な情報）を受信し、そのリソースをRAM 6 3に保持して、処理を終了する。

- 10 この場合、移動端末装置1 1-2は、本親機でない親機1 2-1のリソースを使用することができる。

一方、ステップS 8で、CPU 6 1は、親機1 2-1から権利文を受信していないと判定した場合、ステップS 11に進み、親機1 2-2から、親機1 2-1を介して、リソースを取得する権利を記載した権利文を発行できないことを示すエラー通知を受信したか否かを判定する。ステップS 11で、CPU 6 1は、親機1 2-1からエラー通知を受信していないと判定した場合、ステップS 8に戻り、上述した処理を繰り返す。

また、ステップS 11において、CPU 6 1は、親機1 2-2からエラー通知を受信したと判定した場合、移動端末装置1 1-2は、親機1 2-1に接続しているリソースを取得する権利がないので、処理を終了する。

図4は、図3のステップS 2とステップS 6の共通秘密鍵認証処理を説明するフローチャートである。この処理は、移動端末装置1 1とそのユーザの本親機との間で行われる。

図4の例では、移動端末装置1 1-1における共通秘密鍵認証処理を説明するが、移動端末装置1 1-2における場合も同様の処理が行われる。但し、移動端末装置1 1-2の場合は、本親機である親機1 2-2と無線通信が可能ではないので、無線通信可能な親機1 2-1にその本親機である親機1 2-2のアドレス

を通知し、親機 1 2 - 1 を介して、インターネット 2 1 経由で本親機である親機 1 2 - 2 と通信する。

ステップ S 2 1 において、CPU 6 1 は、リーダライタ 6 5 を制御して、非接触 IC カード 7 1 から、ユーザの認証情報である共通秘密鍵 3 1 を読み込み、RAM 6 3 に保持する。ステップ S 2 1 の処理後は、ステップ S 2 2 に進み、CPU 6 1 は、共通秘密鍵 3 1 を暗号化し、ステップ S 2 3 に進む。即ち、移動端末装置 1 1 - 1 は、認証装置 1 3 から親機 1 2 - 1 (本親機) の秘密鍵 3 5 に対応する公開鍵 3 9 を取得し、RAM 6 3 に保持する。CPU 6 1 は、RAM 6 3 に保持した公開鍵 3 9 を、共通秘密鍵 3 1 とともに暗号/復号部 6 9 に供給する。暗号/復号部 6 9 は、その公開鍵 3 9 を用いて、共通秘密鍵 3 1 を暗号化する。

ステップ S 2 3 では、CPU 6 1 は、ステップ S 2 2 で暗号化した共通秘密鍵 3 1 を、本親機である親機 1 2 - 1 に送信し、ステップ S 2 4 に進む。ステップ S 2 4 において、CPU 6 1 は、親機 1 2 - 1 (本親機) から、後述する図 8 のステップ S 6 4 で送信されてくる秘密鍵 3 5 で暗号化された共通秘密鍵 3 3 を受信したかどうかを判定し、暗号化された共通秘密鍵 3 3 を受信していないと判定した場合、受信されるまで待機する。

ステップ S 2 4 において、CPU 6 1 は、親機 1 2 - 1 から暗号化された共通秘密鍵 3 3 を受信したと判定した場合、ステップ S 2 5 に進み、暗号/復号部 6 9 を制御し、その暗号化された共通秘密鍵 3 3 を、ステップ S 2 2 の処理で RAM 6 3 に保持した、秘密鍵 3 5 と対の公開鍵 3 9 を用いて復号する。このとき、秘密鍵 3 5 とそれに対応する公開鍵 3 9 は、一方の鍵に基づいて生成された暗号文 (パズフレーズ) を他方の鍵を用いて復号できる関係にあるので、秘密鍵 3 5 に基づいて暗号化された共通秘密鍵 3 3 (パズフレーズ) が、親機 1 2 - 1 から送信され、移動端末装置 1 1 - 1 で受信されるまでの間に改ざんされなかった場合、その暗号化された共通秘密鍵 3 3 は、公開鍵 3 9 に基づいて復号されると、共通秘密鍵 3 3 となる。

ステップS 2 5の処理後は、ステップS 2 6に進み、CPU 6 1は、暗号/復号部 6 9を制御して、復号した共通秘密鍵 3 3を、ステップS 2 2の処理でRAM 6 3に保持した公開鍵 3 9を用いて暗号化し、その暗号化した共通秘密鍵を親機 1 2-1（本親機）に送信し、ステップS 2 7に進む。ステップS 2 7において、

5 CPU 6 1は、親機 1 2-1（本親機）から、後述する図 8のステップS 6 8の処理で秘密鍵 3 5を用いて暗号化された共通秘密鍵（親機 1 2-1が、ステップS 2 3で親機 1 2-1に送信された暗号化した共通秘密鍵 3 1を秘密鍵 3 5を用いて復号し、さらに暗号化した共通秘密鍵） 3 1を受信したかどうかを判定する。

ステップS 2 7で、CPU 6 1は、親機 1 2-1から暗号化された共通秘密鍵 3 1を受信したと判定した場合、ステップS 2 8に進み、暗号/復号部 6 9を制御して、その暗号化された共通秘密鍵 3 1を、秘密鍵 3 5と対のRAM 6 3に保持した公開鍵 3 9を用いて復号する。ステップS 2 8の処理後は、ステップS 2 9に進み、ステップS 2 8で復号された共通秘密鍵が、ステップS 2 1でRAM 6 3に保持された共通秘密鍵 3 1と等しいかどうかを判定する。

15 ステップS 2 9において、CPU 6 1は、復号された共通秘密鍵 3 1が、RAM 6 3に保持された共通秘密鍵 3 1と等しいと判定した場合、図 3のステップS 3または図 3のステップS 7にリターンする。即ち、この場合、ステップS 2 3で公開鍵 3 9を用いて暗号化された共通秘密鍵 3 1が、親機 1 2-1により秘密鍵 3 5を用いて正常に復号され、共通秘密鍵 3 1が得られている。そして、その共通

20 秘密鍵 3 1が、親機 1 2-1において秘密鍵 3 5を用いて暗号化され、その暗号化された共通秘密鍵 3 1が、移動端末装置 1 1-1において、公開鍵 3 9を用いて正常に復号され、共通秘密鍵 3 1が得られている。

従って、秘密鍵 3 5とそれに対応する公開鍵 3 9は、一方の鍵に基づいて暗号化された共通秘密鍵 3 1を他方の鍵を用いて復号できる関係にあるので、移動端末装置 1 1-1は、移動端末装置 1 1-1と親機 1 2-1が通信する間で改ざん

25 がなかったことを認識できる。

一方、ステップS 2 9において、CPU 6 1は、ステップS 2 8で復号された共通秘密鍵が、RAM 6 3に保持された共通秘密鍵 3 1と等しくないと判定した場合、秘密鍵 3 5とそれに対応する公開鍵 3 9は、一方の鍵に基づいて生成された共通秘密鍵 3 1を他方の鍵を用いて復号できる関係にないので、移動端末装置 1 1-1と親機 1 2-1が通信する間で改ざんがあった、あるいは、親機 1 2-1が正当な装置でないと認識し、処理を終了する。

このように、移動端末装置 1 1-1は、移動端末装置 1 1-1と親機 1 2-1が通信する間で改ざんがなかったと認識できたときのみ、図3のステップS 3または図3のステップS 7に進み、親機 1 2-1にリソースを要求する信号を送信するので、移動端末装置 1 1-1と親機 1 2-1の両者間での通信中のデータ秘匿が可能となる。

一方、ステップS 2 7において、CPU 6 1は、親機 1 2-1から暗号化された共通秘密鍵 3 1を受信していないと判定した場合、ステップS 3 0に進み、後述する図8のステップS 7 1で親機 1 2-1が送信した、親機 1 2-1と移動端末装置 1 1-1の関係が正当ではないことを示すエラー通知を受信したか否かを判定する。ステップS 3 0において、CPU 6 1は、親機 1 2-1からエラー通知を受信していないと判定した場合、ステップS 2 7に戻り、上述した処理を繰り返す。

一方、ステップS 3 0において、CPU 6 1は、親機 1 2-1からエラー通知を受信したと判定した場合、親機 1 2-1と移動端末装置 1 1-1の関係は正当ではないので、処理を終了する。

図5は、図3のステップS 5の処理を説明するフローチャートである。

ステップS 4 1において、例えば、移動端末装置 1 1-2のCPU 6 1は、直接無線通信することができる本親機でない親機 1 2-1にデバイス探索を要求する。

ステップS 4 1の処理後は、ステップS 4 2に進み、CPU 6 1は、親機 1 2-1から、デバイス探索を許可された（後述する図12のステップS 1 2 1で送信されたデバイス探索許可の通知を受信した）かどうかを判定する。ステップS 4

2 において、CPU 6 1 は、親機 1 2 - 1 からデバイス探索が許可されたと判定した場合、ステップ S 4 3 に進み、親機 1 2 - 1 にリソース情報を要求する。

ステップ S 4 3 の処理後は、ステップ S 4 4 に進み、CPU 6 1 は、リソース情報要求に対応して、親機 1 2 - 1 から送信されたリソース情報を受信し、そのリ
5 ソース情報を RAM 6 3 に保持する。

一方、ステップ S 4 2 において、CPU 6 1 は、親機 1 2 - 1 から、デバイス探索を許可されていないと判定した場合、ステップ S 4 5 に進み、デバイス探索に対応して親機 1 2 - 1 から送信されたデバイス探索の不許可を示すエラー通知が、
10 受信されたかどうかを判定する。ステップ S 4 5 において、CPU 6 1 は、エラー通知が受信されていないと判定した場合、ステップ S 4 2 に戻り、上述した処理を繰り返す。

また、ステップ S 4 5 において、CPU 6 1 は、エラー通知が受信されたと判定した場合、親機 1 2 - 1 にデバイス探索が許可されず、親機 1 2 - 1 からリソース情報を得ることができないので、処理を終了する。

15 図 6 は、図 1 の親機 1 2 の詳細構成例を示している。

図 6 の例では、親機 1 2 - 1 を説明するが、親機 1 2 - 2 も同様に構成される。

親機 1 2 - 1 は、CPU 9 1、ROM 9 2、RAM 9 3、アンテナ 9 4、受信部 9 5、送信部 9 6、入出力部 9 7、データバス 9 8、リソース制御部 9 9、および通信部 1 0 0 から構成されている。

20 CPU 9 1 は、ROM 9 2 に記憶されているプログラムに従って各種の処理を実行する。例えば、CPU 9 1 は、受信部 9 5 から供給された受信データの供給先を判定し、入出力部 9 7 を制御して、その供給先に、受信データを供給する。RAM 9 3 には、CPU 9 1 が各種の処理を実行する上において必要なデータなどが適宜記憶される。

25 アンテナ 9 4 は、移動端末装置 1 1 から送信された信号を受信し、その信号を受信部 9 5 に供給する。また、アンテナ 9 4 は、送信部 9 6 から供給された信号を移動端末装置 1 1 に送信する。

受信部 9 5 は、アンテナ 9 4 から供給された信号を CPU 9 1 に供給する。送信部 9 6 は、CPU 9 1 からの指令に基づいて、移動端末装置 1 1 に送信する信号をアンテナ 9 4 に供給する。

入出力部 9 7 は、データバス 9 8 を介してリソース制御部 9 9 と通信部 1 0 0 に接続されるとともに、リソース機器 1 6 - 1 とリソース機器 1 6 - 2 に接続されている。リソース制御部 9 9 は、リソース機器 1 5 - 1 とリソース機器 1 5 - 2 にそれぞれ接続されている。

通信部 1 0 0 は、CPU 9 1 からの指令に基づき、インターネット 2 1 を介して、親機 1 2 - 2、認証装置 1 3、およびバリュー発行装置 1 4 に信号を送信するとともに、親機 1 2 - 2、認証装置 1 3、およびバリュー発行装置 1 4 から信号を受信する。

図 7 は、図 6 のリソース制御部 9 9 の詳細構成例を示している。

リソース制御部 9 9 は、CPU 1 1 1、ROM 1 1 2、RAM 1 1 3、入出力部 1 1 4、リーダライタ 1 1 5、表示部 1 1 6、および暗号/復号部 1 1 7 から構成される。

15 CPU 1 1 1 は、ROM 1 1 2 に記憶されているプログラムに従って各種の処理を実行する。RAM 1 1 3 は、ユーザの個人情報を格納しており、CPU 1 1 1 は、個人情報を管理している。また、RAM 1 1 3 には、CPU 1 1 1 が各種の処理を実行する上において必要なデータなどが適宜記憶される。

CPU 1 1 1 は、入出力部 1 1 4 を介して、リソース機器 1 5 - 1 とリソース機器 1 5 - 2 に接続されており、リソース機器 1 5 - 1 とリソース機器 1 5 - 2 から供給されたリソースを、データバス 9 8 および入出力部 9 7 を介して、CPU 9 1 に供給する。リーダライタ 1 1 5 は、親機 1 2 - 1 に備えられた非接触 IC カード 1 2 1 から、データを読み込んだり、データを書き込む。

非接触 IC カード 1 2 1 には、個人認証用の情報の格納領域と電子バリューのための認証用の情報の格納領域が設けられている。個人認証用の情報の格納領域には、移動端末装置 1 1 - 1 の共通秘密鍵 3 1 と同一の共通秘密鍵 3 3 と自らの正当性を証明するための秘密鍵 3 5 が格納されている。電子バリューのための認

証用の情報の格納領域には、バリュー発行装置 1 4 により発行された共通秘密鍵 3 4 等が格納されている。なお、電子バリューのための認証用の情報の格納領域は、認証用と電子バリュー用の領域に分けることができる。認証用の領域には、秘密鍵 3 4 が格納され、電子バリューの領域には、電子バリュー（例えば、権利
5 文）が格納される。

このように、共通秘密鍵 3 3、共通秘密鍵 3 4、および秘密鍵 3 5 を改ざんが困難な非接触 IC カード 1 2 1 に安全に格納することにより、通信システムの安全性と利便性を向上させることができる。

表示部 1 1 6 は、CPU 1 1 1 の指令により、例えば、リソース情報を表示する。

10 暗号/復号部 1 1 7 は、鍵、その他の情報を暗号化または復号する。

なお、親機 1 2 - 1 は、物理的に 1 つの筐体で構成する必要はなく、データベースを経由して複数の機器が協調して機能を実現するように構成してもよい。

図 8 は、図 7 の親機 1 2 のリソース制御部 9 9 がリソースを制御する処理を説明するフローチャートである。この処理は、例えば、移動端末装置 1 1 から信号
15 を受信したとき開始される。

以下の説明では、親機 1 2 - 1 がリソースを制御する処理を説明するが、親機 1 2 - 2 における場合も同様の処理が行われる。

ステップ S 6 1 では、CPU 1 1 1 は、リーダライタ 1 1 5 を制御し、非接触 IC カード 1 2 1 から共通秘密鍵 3 3 を読み込み、その共通秘密鍵 3 3 を RAM 1 1
20 3 に保持する。ステップ S 6 1 の処理後は、ステップ S 6 2 に進み、CPU 1 1 1 は、図 4 のステップ S 2 3 で移動端末装置 1 1 - 1 から送信された暗号化した共通秘密鍵 3 1 が受信されたかどうかを判定する。

即ち、CPU 9 1 は、アンテナ 9 4 により受信され、受信部 9 5 を介して供給された信号が、親機 1 2 - 1 に対するものである場合、入出力部 9 7 を制御し、
25 データバス 9 8 を介して、その信号をリソース制御部 9 9 の CPU 1 1 1 に供給し、CPU 1 1 1 は、その信号が暗号化された共通秘密鍵 3 1 であるかどうかを判定する。なお、以下の説明では、このように CPU 9 1 がアンテナ 9 4 により受信され

た信号をリソース制御部 99 の CPU 111 に供給することを、単に、CPU 111 が信号を受信するという。

ステップ S 6 2 において、CPU 111 は、移動端末装置 11-1 から暗号化された共通秘密鍵 31 が受信されたと判定した場合、ステップ S 6 3 に進み、非接触 IC カード 121 から秘密鍵 35 を読み込み、その暗号化された共通秘密鍵 31 と秘密鍵 35 を RAM 113 に保持する。そして、CPU 111 は、暗号/復号部 117 を制御し、ステップ S 6 1 で RAM 113 に保持した共通秘密鍵 33 を、秘密鍵 35 を用いて暗号化する。

ステップ S 6 3 の処理後は、ステップ S 6 4 に進み、CPU 111 は、ステップ S 6 2 で暗号化された共通秘密鍵 33 を、移動端末装置 11-1 に送信し、ステップ S 6 4 からステップ S 6 5 に進む。ステップ S 6 5 では、CPU 111 は、図 4 のステップ S 26 で移動端末装置 11-1 から送信された暗号化された共通秘密鍵が受信されたかどうかを判定し、移動端末装置 11-1 から暗号化された共通秘密鍵が受信されるまで待機する。

ステップ S 6 5 において、CPU 111 は、移動端末装置 11-1 から暗号化された共通秘密鍵が供給されたと判定した場合、ステップ S 6 6 に進み、その暗号化された共通秘密鍵を復号し、ステップ S 6 7 に進む。即ち、CPU 111 は、暗号/復号部 117 を制御し、ステップ S 6 3 で RAM 113 に保持した、公開鍵 39 と対の秘密鍵 35 を用いて、暗号化された共通秘密鍵を復号する。

ステップ S 6 7 では、CPU 111 は、その復号された共通秘密鍵が、RAM 113 に保持された共通秘密鍵 33 と等しいかどうかを判定する。ステップ S 6 7 において、CPU 111 は、その復号された共通秘密鍵が RAM 113 に保持された共通秘密鍵 33 と等しいと判定した場合、ステップ S 6 8 に進む。

即ち、この場合、ステップ S 6 3 で秘密鍵 35 を用いて暗号化された共通秘密鍵 33 が、移動端末装置 11-1 において、公開鍵 39 を用いて正常に復号され、共通秘密鍵 33 が得られている。そして、その秘密鍵 33 が移動端末装置 11-1 において、公開鍵 39 を用いて暗号化され、その暗号化された共通秘密鍵 3

1 が、親機 1 2 - 1 において、秘密鍵 3 5 を用いて正常に復号され、共通秘密鍵 3 3 が得られている。

従って、秘密鍵 3 5 とそれに対応する公開鍵 3 9 は、一方の鍵に基づいて暗号化された共通秘密鍵 3 3 を他方の鍵を用いて復号できる関係にあるので、親機 1 2 - 1 は、移動端末装置 1 1 - 1 と親機 1 2 - 1 が通信する間で改ざんがなかったことが認識できる。

その後、ステップ S 6 8 において、CPU 1 1 1 は、ステップ S 6 2 で移動端末装置 1 1 - 1 から受信し、RAM 1 1 3 に保持した暗号化された共通秘密鍵 3 1 を、RAM 1 1 3 に保持した公開鍵 3 9 と対の秘密鍵 3 5 を用いて復号する。

10 ステップ S 6 8 の処理後は、ステップ S 6 9 に進み、CPU 1 1 1 は、ステップ S 6 8 で復号した共通秘密鍵が、RAM 1 1 3 に保持した共通秘密鍵 3 3 と等しいかどうかを判定する。ステップ S 6 9 において、CPU 1 1 1 は、その復号した共通秘密鍵が RAM 1 1 3 に保持した共通秘密鍵 3 3 と等しいと判定した場合、ステップ S 7 0 に進む。

15 即ち、この場合、図 4 のステップ S 2 2 で移動端末装置 1 1 - 1 により公開鍵 3 9 を用いて暗号化された、秘密鍵 3 3 と同一の共通秘密鍵 3 1 が、ステップ S 6 8 で親機 1 2 - 1 により秘密鍵 3 5 を用いて正常に復号され、共通秘密鍵 3 1 が得られている。そして、移動端末装置 1 1 - 1 が有する共通秘密鍵 3 1 と親機 1 2 - 1 が有する共通秘密鍵 3 3 が同一であることが検証、つまり、移動端末装置 1 1 - 1 のユーザが、親機 1 2 - 1 のユーザであることが検証されている。

従って、秘密鍵 3 5 とそれに対応する公開鍵 3 9 は、一方の鍵に基づいて暗号化された共通秘密鍵 3 1 を他方の鍵を用いて復号できる関係にあるので、親機 1 2 - 1 は、移動端末装置 1 1 - 1 と親機 1 2 - 1 が通信する間で改ざんがなかったことが認識できる。また、移動端末装置 1 1 - 1 が有する共通秘密鍵 3 1 と親機 1 2 - 1 が有する共通秘密鍵 3 3 が等しくなっているので、親機 1 2 - 1 は、移動端末装置 1 1 - 1 のユーザが個人情報情報を格納したユーザであることを認識する。

その後、ステップS 7 0において、暗号/復号部6 9を制御して、その復号した共通秘密鍵を、RAM 1 1 3に保持した秘密鍵3 5を用いて暗号化し、移動端末装置1 1 - 1に送信する。

一方、ステップS 6 7において、CPU 1 1 1は、ステップS 6 6で復号された
5 共通秘密鍵が RAM 1 1 3に保持する共通秘密鍵3 3と等しくないと判定した場合、
またはステップS 6 9で、ステップS 6 8で復号された共通秘密鍵が RAM 1 1 3
に保持する共通秘密鍵3 3と等しくないと判定した場合、移動端末装置1 1 - 1
と親機1 2 - 1が通信する間で改ざんがあったか、または親機1 2 - 1が移動端
末装置1 1 - 1の本親機ではないので、ステップS 7 1に進み、移動端末装置1
10 1 - 1と親機1 2 - 1の関係が正当ではないことを示すエラー通知を送信し、処
理を終了する。

このように、親機1 2 - 1は、移動端末装置1 1 - 1と親機1 2 - 1が通信する
間で改ざんがなく、かつ移動端末装置1 1 - 1の本親機であると認識できたとき
のみ、復号した共通秘密鍵3 1を暗号化して移動端末装置1 1 - 1に送信する。

15 この後、移動端末装置1 1 - 1は、移動端末装置1 1 - 1と親機1 2 - 1が通
信する間で改ざんがなかったと認識できたときのみリソースを要求する信号を親
機1 2 - 1に送信するので、移動端末装置1 1 - 1は、移動端末装置1 1 - 1と
親機1 2 - 1が通信する間で改ざんがなかったと移動端末装置1 1 - 1と親機1
2 - 1の両方で認識（双方向認証）され、かつ親機1 2 - 1が移動端末装置1 1
20 - 1の本親機である場合のみ、リソースを要求し、利用することができる。

これにより、移動端末装置1 1 - 1と親機1 2 - 1の両者間での通信中のデー
タ秘匿が可能となる。

ステップS 6 2において、CPU 1 1 1は、移動端末装置1 1 - 1からリソース
要求信号が供給されたと判定した場合、ステップS 7 3に進み、リソース送信処
25 理を行い、その後、処理を終了する。リソース送信処理の詳細は、図9と図10
で後述する。

一方、ステップS 7 2において、CPU 1 1 1は、リソース要求信号が供給されていないと判定した場合、ステップS 6 2に戻り、上述した処理を繰り返す。

図9は、移動端末装置1 1-1および1 1-2と直接無線通信が可能な親機1 2-1が図8のステップS 7 3の処理で行うリソース送信処理を説明するフローチャートである。

ステップS 8 1において、親機1 2-1のCPU 1 1 1は、図8のステップS 7 2で受信したリソース要求信号が自身が本親機となる移動端末装置（移動端末装置1 1-1）からのリソース要求信号であるかどうかを判定する。ステップS 8 1において、親機1 2-1のCPU 1 1 1は、受信したリソース要求信号が自身が
10 本親機となる移動端末装置1 1-1からのリソース要求信号であると判定した場合、ステップS 8 2をスキップしてステップS 8 3に進む。

ステップS 8 3では、親機1 2-1のCPU 1 1 1は、入出力部1 1 4を制御し、移動端末装置1 1-1からのリソース要求信号に基づいて、移動端末装置1 1-1から要求されているリソースを有するリソース機器1 5からリソースを取得し、
15 ステップS 8 4に進む。ステップS 8 4では、親機1 2-1のCPU 1 1 1は、そのリソースを、移動端末装置1 1-1に送信してリターンする。

即ち、親機1 2-1は、個人情報格納しているユーザが使用する移動端末装置1 1-1から、親機1 2-1の接続するリソース機器1 5の有するリソースを要求された場合、無条件に利用を許可する。

20 一方、ステップS 8 1において、親機1 2-1のCPU 1 1 1は、図8のステップS 7 2で受信したリソース要求信号が、自身が本親機とならない移動端末装置からのリソース要求信号である（移動端末装置1 1-2からのリソース要求信号である）と判定した場合、ステップS 8 2に進み、権利文の提示がある（リソース要求信号とともに権利文が送信されてきた）かどうかを判定する。ステップS
25 8 2において、親機1 2-1のCPU 1 1 1は、権利文の提示がなかったと判定した場合、移動端末装置1 1-2はリソースを利用する権利がないので、処理を終了する。

ステップS 8 2において、親機1 2－1のCPU 1 1 1は、権利文の提示があったと判定した場合、ステップS 8 3に進み、入出力部1 1 4を制御し、移動端末装置1 1－2からのリソース要求信号に基づいて、移動端末装置1 1－2から要求されているリソースを有するリソース機器1 5からリソースを取得し、ステップS 8 4に進む。ステップS 8 4では、親機1 2－1のCPU 1 1 1は、そのリソースを、移動端末装置1 1－2に送信する。

即ち、親機1 2－1は、個人情報を格納していないユーザが使用する移動端末装置1 1－2から、親機1 2－1に接続しているリソース機器1 5の有するリソースを要求された場合、移動端末装置1 1－2がリソースを利用する権利文を取得している場合のみ、リソース利用を許可する。逆に言えば、移動端末装置1 1－2のユーザは、本親機1 2－1のリソースを、そのリソースを利用する権利文を、親機1 2－1に提示したときのみ利用することができる。

なお、親機1 2－1は、親機1 2－2が移動端末装置1 1－2のユーザを認証するときのやりとり時に、移動端末装置1 1－2は、そのユーザの個人情報を、その本親機である親機1 2－2から取得する。ここで、個人情報には、そのユーザがリソースを利用したときの操作履歴などが含まれる。即ち、移動端末装置1 1－2の本親機である親機1 2－2は、例えば、そのユーザが自身の有するリソースを利用したときに、その利用時の操作履歴などを個人情報として登録する個人情報管理機能を有する。移動端末装置1 1－2は、親機1 2－1のリソースを利用するときに、ユーザの個人情報に応じて、移動端末装置1 1－2のユーザの嗜好に合わせた操作性（ユーザI／F）を提供する。

図1 0は、移動端末装置1 1－2がその本親機である親機1 2－2と直接無線通信できない場合に、その親機1 2－2が図8のステップS 7 1の処理で行うリソース送信処理を説明するフローチャートである。なお、親機1 2－2は、認証装置1 3から発行された電子証明書（図1 1で後述する）を既に受信し、RAM 1 1 3に保持しているものとする。

ステップS 1 0 0において、親機1 2 - 2のCPU 1 1 1は、暗号化した利用権発行要求文と、RAM 1 1 3に保持している電子証明書を作成し、その利用権発行要求文と電子証明書を、移動端末装置1 1 - 1がリソースを利用しようとする本親機でない親機1 2 - 1に送信する。即ち、親機1 2 - 2のCPU 1 1 1は、直接
5 無線通信することができない移動端末装置1 1 - 2から送信されたリソース要求信号に基づいて、リソース情報の識別子と利用方法を明記した利用権発行要求文を作成する。

また、親機1 2 - 2のCPU 1 1 1は、リーダライタ1 1 5を制御し、非接触I Cカード1 2 1から読み込んだ秘密鍵3 8をRAM 1 1 3に保持する。CPU 1 1 1
10 は、暗号/復号部1 1 7を制御し、RAM 1 1 3に保持した秘密鍵3 8を用いて、電子署名を暗号化し、利用権発行要求文を付加する。そして、CPU 1 1 1は、その利用権発行要求文を電子証明書とともに、移動端末装置1 1 - 2がリソースを利用しようとしている親機1 2 - 1に送信する。

なお、利用権発行要求文とは、ここでは、移動端末装置1 1 - 2が、その本親
15 機でない親機1 2 - 1のリソースの利用をするための利用権の発行を、親機1 2 - 1に要求するメッセージである。

また、移動端末装置1 1 - 2が本親機である親機1 2 - 2に送信するリソース要求信号には、その移動端末装置1 1 - 2がリソースを利用しようとする本親機でない親機1 2 - 2へアクセスするためのアクセス情報が含まれている。そして、
20 親機1 2 - 2は、このアクセス情報に基づいて、利用権発行要求文を親機1 2 - 1に送信する。

ステップS 1 0 0の処理後は、ステップS 1 0 1に進み、親機1 2 - 2のCPU 1 1 1は、後述する図1 3のステップS 1 4 7で、利用権発行要求文を受信した親機1 2 - 1が親機1 2 - 2に対して送信するリソースの利用を許可するための
25 対価（バリュー）と対価の送信先口座情報を記載したリソース利用条件文と電子証明書を受信したかどうかを判定する。ステップS 1 0 1において、親機1 2 - 2のCPU 1 1 1は、リソース利用条件文と電子証明書を受信したと判定した場合、

暗号/復号部 117 を制御し、電子証明書に含まれる、親機 12-1 の秘密鍵 35 に対応する公開鍵 39 を用いて、リソース利用条件文に含まれる電子署名を復号し、ステップ S101 からステップ S102 に進む。

5 ステップ S102 において、親機 12-2 の CPU 111 は、リソース利用条件文が正当であるかどうかを判定する。即ち、CPU 111 は、リソース利用条件文に含まれる電子署名が正常に復号されたかどうかを判定する。ステップ S102 において、CPU 111 は、リソース利用条件文が正当ではないと判定した場合、親機 12-1 の秘密鍵 35 で暗号化された電子署名が、それと対の公開鍵 39 で復号できていないので、親機 12-1 と親機 12-2 が通信する間で改ざんが行
10 われたと判定し、処理を終了する。

 また、ステップ S102 において、親機 12-2 の CPU 111 は、リソース利用条件文が正当であると判定した場合、秘密鍵 35 で暗号化された電子署名が、公開鍵 39 で復号できるので、親機 12-1 と親機 12-2 が通信する間で改ざんが行われず、親機 12-1 と親機 12-2 が正当な関係であると認識し、ステ
15 ップ S102 からステップ S103 に進む。

 このように、電子署名を用いてリソース利用条件文が正当であるかどうかを判定することにより、通信システム 1 の安全性をさらに高めることができる。

 ステップ S103 において、親機 12-2 の CPU 111 は、リソース利用条件文に基づいて、親機 12-2 から親機 12-1 にバリューを移動する（対価を支
20 払う）ためのバリュー移動要求をバリュー発行装置 14 に送信する。

 ステップ S103 の処理後は、ステップ S104 に進み、親機 12-2 の CPU 111 は、バリュー発行装置 14 から、後述する図 16 のステップ S162 で送信される暗号化された共通秘密鍵 44 を受信したかどうかを判定する。ステップ S104 において、CPU 111 は、バリュー発行装置 14 から暗号化された共通
25 秘密鍵 44 を受信していないと判定した場合、バリュー発行装置 14 から暗号化された共通秘密鍵 44 が受信されるまで待機する。

ステップS 1 0 4において、親機1 2-2のCPU1 1 1は、バリュウ発行装置1 4から暗号化された共通秘密鍵4 4を受信したと判定した場合、ステップS 1 0 5に進み、親機1 2-2のCPU1 1 1は、バリュウ発行装置1 4の有する秘密鍵4 3に対応する公開鍵4 1を、認証装置1 3から取得し、RAM1 1 3に保持する。そして、親機1 2-2のCPU1 1 1は、暗号/復号部1 1 7を制御し、RAM1 1 3に保持した公開鍵4 1を用いて、暗号化された共通秘密鍵4 4を復号し、復号した共通秘密鍵4 4をRAM1 1 3に保持する。

ステップS 1 0 5の処理後は、ステップS 1 0 6に進み、親機1 2-2のCPU1 1 1は、リーダライタ1 1 5を制御して、共通秘密鍵3 7を読み込み、RAM1 1 3に保持し、ステップS 1 0 7に進む。ステップS 1 0 7では、親機1 2-2のCPU1 1 1は、RAM1 1 3から復号した共通秘密鍵4 4と共通秘密鍵3 7を読み出し、両者が等しいかどうかを判定する。

ステップS 1 0 7において、親機1 2-2のCPU1 1 1は、復号した共通秘密鍵4 4と共通秘密鍵3 7が等しいと判定した場合、即ち、後述する図1 6のステップS 1 6 1でバリュウ発行装置1 4により秘密鍵4 3を用いて暗号化された共通秘密鍵4 4が、ステップS 1 0 6で親機1 2-2により公開鍵4 1を用いて正常に復号され、共通秘密鍵3 7と等しい共通秘密鍵4 4が得られている場合、親機1 2-2のCPU1 1 1は、バリュウ発行装置1 4と親機1 2-2が通信する間で改ざんがなかったことが認識し、ステップS 1 0 7からステップS 1 0 8に進む。

従って、CPU1 1 1は、S 1 0 8では、親機1 2-2のCPU1 1 1は、暗号/復号部1 1 7を制御し、RAM1 1 3に保持した公開鍵4 1を用いて、RAM1 1 3に保持した共通秘密鍵3 7を暗号化する。ステップS 1 0 9の処理後は、ステップS 1 1 0に進み、親機1 2-2のCPU1 1 1は、その暗号化した共通秘密鍵3 7を、バリュウ発行装置1 4に送信し、リターンする。

一方、ステップS 1 0 7において、親機1 2-2のCPU1 1 1は、ステップS 1 0 6で復号した共通秘密鍵と共通秘密鍵3 4が等しくないと判定した場合、

バリュ発行装置 1 4 と親機 1 2 - 2 が通信する間で改ざんがあったと認識し、ステップ S 1 1 0 に進み、バリュ発行装置 1 4 に、バリュ発行装置 1 4 と親機 1 2 - 2 の関係は正当ではないことを示すエラーを通知してリターンする。

また、ステップ S 1 0 1 において、親機 1 2 - 2 の CPU 1 1 1 は、移動端末装置 1 2 - 2 がリソースを利用しようとする親機 1 2 - 1 からのリソース利用条件文を受信していないと判定した場合、ステップ S 1 1 1 に進み、親機 1 2 - 1 から、後述する図 1 3 のステップ S 1 4 8 で送信されたるリソース利用条件文を発行できないことを示すエラー通知を受信したかどうかを判定する。ステップ S 1 1 0 において、親機 1 2 - 2 の CPU 1 1 1 は、親機 1 2 - 1 からエラー通知を受信していないと判定した場合、ステップ S 1 0 1 に戻り、上述した処理を繰り返す。

また、ステップ S 1 1 1 において、親機 1 2 - 2 の CPU 1 1 1 は、親機 1 2 - 1 からエラー通知を受信したと判定した場合、即ち、親機 1 2 - 1 がリソース利用条件文を発行せず、移動端末装置 1 1 - 2 によるリース利用を許可しなかった場合、処理を終了する。

図 1 1 は、電子証明書の例を示す図である。

この電子証明書は、図 1 1 に示されるように、証明書のバージョン番号、証明書の通し番号、署名に用いたアルゴリズムとパラメータ、認証装置 1 3 の名前、証明書の有効期限、発行された装置の ID、および装置の公開鍵が含まれている。

この電子証明書は、認証装置 1 3 により、親機 1 2 - 1、親機 1 2 - 2、およびバリュ発行装置 1 4 に対して発行される。親機 1 2 - 1、親機 1 2 - 2、およびバリュ発行装置 1 4 は、自らの正当性を証明するために他の装置に、暗号文とともにこの電子証明書を送信する。受信した装置は、この電子証明書に含まれる装置の公開鍵を用いて、この電子証明書とともに送信されてくる暗号文を復号し、その暗号文の正当性を認識することができる。

図 1 2 は、図 6 の親機 1 2 - 1 がリソース情報を送信する処理を説明するフローチャートである。この処理は、例えば、親機 1 2 - 1 が図 5 のステップ S 4 1

で移動端末装置 11-2 から送信されるブロードキャスト要求信号を受信したとき開始される。

ステップ S 120 において、親機 12-1 の CPU 91 は、移動端末装置 11-2 によるブロードキャスト要求を許可するかどうかを判定する。ステップ S 120 において、親機 12-1 の CPU 91 は、ブロードキャスト要求を許可すると判定した場合、ステップ S 121 に進み、移動端末装置 11-2 にブロードキャスト要求許可の通知を送信する。

ステップ S 121 の処理後は、ステップ S 122 に進み、親機 12-1 の CPU 91 は、移動端末装置 11-2 から図 5 のステップ S 43 でリソース情報要求信号が送信されて来るのを待って受信し、ステップ S 123 に進む。

ステップ S 123 において、親機 12-1 の CPU 91 は、入出力部 97 を制御し、データバス 98 とリソース制御部 99 を介して、リソース機器 15-1 とリソース機器 15-2 から、移動端末装置 12-2 に提供することができる、または提供してもよいリソースのリソース情報を取得する。同様に、CPU 91 は、入出力部 97 を制御し、データバス 98 を介して、リソース機器 16-1 とリソース機器 16-2 からリソース情報を取得する。そして、CPU 91 は、取得したリソース情報を移動端末装置 11-2 に送信して処理を終了する。

一方、ステップ S 120 において、CPU 91 は、移動端末装置 11-2 からのブロードキャスト要求を許可しないと判定した場合、ステップ S 124 に進み、移動端末装置 11 にブロードキャスト要求を許可しないことを示すエラー通知を送信し、処理を終了する。

図 13 は、図 6 の親機 12-1 が、リソース利用条件文を発行するときに行うリソース利用条件文発行処理を説明するフローチャートである。この処理は、親機 12-1 が図 10 のステップ S 100 の処理で親機 12-2 から送信された、暗号化された利用権発行要求文と電子証明書を受信したとき開始される。なお、親機 12-1 は、認証装置 13 から発行された電子証明書（図 11）を既に受信し、RAM 113 に保持しているものとする。

ステップS 1 4 1において、親機1 2－1のCPU 1 1 1は、親機1 2－2から
利用権発行要求文とともに受信した電子証明書から公開鍵4 0を取得し、ステッ
プS 1 4 2に進む。ステップS 1 4 2では、親機1 2－1のCPU 1 1 1は、親機
1 2－2から受信した利用権発行要求文から秘密鍵3 8を用いて暗号化された電
5 子署名を取得する。CPU 1 1 1は、暗号/復号部1 1 7を制御して、電子署名を、
ステップS 1 4 1で取得した、秘密鍵3 8と対の公開鍵4 0を用いて復号する。

ステップS 1 4 2の処理後は、ステップS 1 4 3に進み、親機1 2－1のCPU
1 1 1は、利用権発行要求文が正当であるかどうかを判定する。即ち、親機1 2
－1のCPU 1 1 1は、ステップS 1 4 2で電子署名が正常に復号されたかどうか
10 を判定し、電子署名が正常に復号された場合、秘密鍵3 8で暗号化された電子署
名が、秘密鍵3 8に対応する公開鍵4 0で正常に復号されているので、親機1 2
－1と親機1 2－2が通信する間で改ざんが行われていないと認識し、利用権発
行要求文が正当であると判定する。

ステップS 1 4 3において、親機1 2－1のCPU 1 1 1は、利用権発行要求文
15 が正当ではないと判定した場合、リソース利用を許可することはできないので、
ステップS 1 4 8に進み、リソース利用の不許可を示すエラー通知を送信して処
理を終了する。

ステップS 1 4 3において、親機1 2－1のCPU 1 1 1は、利用権発行要求文
が正当であると判定した場合、ステップS 1 4 4に進み、親機1 2－2から受信
20 した電子証明書が有効であるかどうかの判定を要求する評価要求信号を、認証装
置1 3に送信し、ステップS 1 4 5に進む。

ステップS 1 4 5では、親機1 2－1のCPU 1 1 1は、認証装置1 3から、図
1 8のステップS 1 8 3またはステップS 1 8 4で送信される電子証明書の評価
を受信したかどうかを判定し、電子証明書の評価を受信していないと判定した場
25 合、電子証明書の評価を受信するまで待機する。

ステップS 1 4 5において、親機1 2－1のCPU 1 1 1は、認証装置1 3から
電子証明書の対価を受信したと判定した場合、ステップS 1 4 6に進み、その認

証装置 1 3 からの電子証明書の評価が有効であるかどうかを判定する。ステップ S 1 4 6 において、親機 1 2 - 1 の CPU 1 1 1 は、認証装置 1 3 から電子証明書は有効であるという評価を受信したと判定した場合、即ち、利用件発行要求とともに送信されてきた電子証明書が失効していない（無効でない）場合、ステップ 5 S 1 4 7 に進み、リソース利用を許可するための対価を記載したリソース利用条件文を電子的に作成する。

このとき、親機 1 2 - 1 の CPU 1 1 1 は、暗号/復号部 1 1 7 を制御して、自らの正当性を証明するために、秘密鍵 3 5 を用いて電子署名を暗号化し、リソース利用条件文に電子署名を付加する。そして、CPU 1 1 1 は、電子署名を付加した利用条件文と、RAM 1 1 3 に保持した電子証明書を、親機 1 2 - 2 に送信し、10 処理を終了する。

一方、ステップ S 1 4 6 において、親機 1 2 - 1 の CPU 1 1 1 は、認証装置 1 3 から電子証明書は有効ではない（無効である）という評価を受信したと判定した場合、リソース利用を許可することはできないので、ステップ S 1 4 8 に進み、15 リソース利用の不許可を示すエラー通知を親機 1 2 - 2 に送信し、処理を終了する。

なお、親機 1 2 - 1 がリソースを利用する権利を記載した権利文を発行する処理も、図 1 3 と同様に行われる。但し、この権利文を発行する処理は、バリュ
ュー発行装置 1 4 から、後述する図 1 6 のステップ S 1 6 8 で送信される暗号化
20 された振込み通知書と電子証明書を受信したとき開始される。

即ち、図 1 4 は、図 6 の親機 1 2 - 1 がリソースを利用するための権利文を発行するときに行う権利文発行処理を説明するフローチャートである。この処理は、親機 1 2 - 1 が後述する図 1 6 のステップ S 1 6 8 の処理でバリュ
ュー発行装置 1 4 から送信される、振込み通知書と電子証明書を受信したとき開始される。なお、
25 親機 1 2 - 1 は、認証装置 1 3 から発行された電子証明書（図 1 1）を既に受信し、RAM 1 1 3 に保持しているものとする。

ステップS 1 5 1において、親機1 2-1のCPU 1 1 1は、バリュー発行装置1 4から、振り込み通知書とともに受信した電子証明書から公開鍵4 1を取得し、ステップS 1 5 2に進む。ステップS 1 5 2では、親機1 2-1のCPU 1 1 1は、バリュー発行装置1 4から受信した振り込み通知書から秘密鍵4 3を用いて暗号化された電子署名を取得する。親機1 2-1のCPU 1 1 1は、暗号/復号部1 1 7を制御して、電子署名を、ステップS 1 5 1で取得した公開鍵4 1を用いて復号する。

ステップS 1 5 2の処理後は、ステップS 1 5 3に進み、親機1 2-1のCPU 1 1 1は、振り込み通知書が正当であるかどうかを判定する。即ち、CPU 1 1 1は、電子署名が正常に復号されたかどうかを判定し、電子署名が正常に復号された場合、秘密鍵4 3で暗号化された電子署名が、秘密鍵4 3に対応する公開鍵4 1で正常に復号されているので、親機1 2-1とバリュー発行装置1 4が通信する間で改ざんが行われていないと認識し、振り込み通知書が正当であると判定する。

ステップS 1 5 3において、親機1 2-1のCPU 1 1 1は、振り込み通知書が正当ではないと判定した場合、リソース利用を許可することはできないので、ステップS 1 5 8に進み、リソース利用の不許可を示すエラー通知を送信して処理を終了する。

また、ステップS 1 5 3において、親機1 2-1のCPU 1 1 1は、振り込み通知書が正当であると判定した場合、ステップS 1 5 4に進み、バリュー発行装置1 4から受信した電子証明書が有効であるかどうかの判定を要求する評価要求信号を、認証装置1 3に送信し、ステップS 1 5 5に進む。

ステップS 1 5 5では、親機1 2-1のCPU 1 1 1は、認証装置1 3から、後述する図1 8のステップS 1 8 3またはステップS 1 8 4で送信される電子証明書の評価を受信したかどうかを判定し、電子証明書の評価を受信していないと判定した場合、電子証明書の評価を受信するまで待機する。

そして、ステップS 1 5 5において、親機1 2-1のCPU 1 1 1は、認証装置1 3から電子証明書の評価を受信したと判定した場合、ステップS 1 5 6に進み、

CPU 1 1 1 は、認証装置 1 3 から電子証明書は有効であるという評価を受信したかどうかを判定する。ステップ S 1 5 6 において、CPU 1 1 1 は、認証装置 1 3 から電子証明書は有効であるという評価を受信したと判定した場合、ステップ S 1 5 7 に進み、リソースを利用する権利を記載した権利文を電子的に作成する。

- 5 このとき、親機 1 2 - 1 の CPU 1 1 1 は、暗号/復号部 1 1 7 を制御して、自らの正当性を証明するために、秘密鍵 3 5 を用いて電子署名を暗号化し、権利文に電子署名を付加する。そして、親機 1 2 - 1 の CPU 1 1 1 は、電子署名を付加した権利文と、RAM 1 1 3 に保持した電子証明書を、親機 1 2 - 2 に送信して処理を終了する。

- 10 一方、ステップ S 1 5 6 において、親機 1 2 - 1 の CPU 1 1 1 は、認証装置 1 3 から電子証明書は有効ではない（無効である）という評価を受信したと判定した場合、リソース利用を許可することはできないので、ステップ S 1 5 8 に進み、リソース利用の不許可を示すエラー通知を親機 1 2 - 2 に送信して処理を終了する。

- 15 図 1 5 は、図 1 のバリュウ発行装置 1 4 の詳細構成例である。

バリュウ発行装置 1 4 は、通信部 1 3 1、データバス 1 3 2、共通秘密鍵認証部 1 3 3、公開鍵認証部 1 3 4、バリュウ発行部 1 3 5、共通秘密鍵記憶部 1 3 6、秘密鍵記憶部 1 3 7、証明書記憶部 1 3 8、発行履歴記憶部 1 3 9、およびバリュウ記憶部 1 4 0 から構成されている。

- 20 通信部 1 3 1 は、インターネット 2 1 を介して、親機 1 2 - 1、親機 1 2 - 2、および認証装置 1 3 からの信号を受信するとともに、親機 1 2 - 1、親機 1 2 - 2、および認証装置 1 3 に信号を送信する。通信部 1 3 1 は、データバス 1 3 2 を介して、共通秘密鍵認証部 1 3 3、公開鍵認証部 1 3 4、およびバリュウ発行部 1 3 5 に接続されている。

- 25 共通秘密鍵認証部 1 3 3 は、共通秘密鍵記憶部 1 3 6 に記憶された共通秘密鍵 4 4 に基づいて、バリュウ発行装置 1 4 にアクセスしてきた親機 1 2 が正当であるかどうかを判定する。また、共通秘密鍵認証部 1 3 3 は、バリュウ発行装置 1

4 がバリューを管理する親機 1 2 に対して、共通秘密鍵 4 4 と同一の秘密鍵 3 4 または 3 7 を送信し、親機 1 2 の非接触 IC カード 1 2 1 に記憶させる。

5 このように、親機 1 2 の非接触 IC カード 1 2 1 にバリュー発行装置 1 4 の共通秘密鍵 4 4 と等しい共通秘密鍵 3 4 または 3 7 を記憶させることにより、親機 1 2 とバリュー発行装置 1 4 との間での認証が可能となり、ユーザが、その親機 1 2 と通信が可能な移動端末装置 1 1 を使用するだけで、バリュー発行装置 1 4 を介して、親機 1 2 どちらの間でのバリューの移動をすることができる。

公開鍵認証部 1 3 4 は、秘密鍵記憶部 1 3 7 に記憶された秘密鍵 4 3 や、証明書記憶部 1 3 8 に記憶された電子証明書を用いて、親機 1 2 - 1、親機 1 2 - 2、
10 および認証装置 1 3 との間で通信部 1 3 1 を開始、公開鍵暗号系の処理を行なう。

バリュー発行部 1 3 5 は、バリュー記憶部 1 4 0 に記憶されたバリュー（電子バリュー）に基づき、バリューを発行し、その発行履歴を発行履歴記憶部 1 3 9 に記憶させる。

15 なお、バリュー発行装置 1 4 は、物理的に 1 つの筐体に入る必要はなく、データバス 1.3 2 を経由して複数の機器が協調して機能を実現してもよい。

また、バリュー発行装置 1 4 は、発行したバリューに応じた対価を決済できるようにしてもよい。さらに、親機 1 2 は、所有する電子バリューをネットワークでの決済に使用してもよい。

20 また、電子バリューの形式は何でもよい。電子バリューはバリュー発行装置 1 4 のバリュー記憶部 1 4 0 に口座という形で格納してもよい。この場合、より高い安全性を提供することができる。

口座を表す ID は、親機の証明書にある機器 ID、あるいはそれに対応させた別の ID を用いることにより、ユーザは個人情報に結びつかない匿名性の高い口座を持つことができる。

25 さらに、バリューは、バリュー発行装置 1 4 のバリュー記憶部 1 4 0 に口座という形で記憶されるだけでなく、親機 1 2 の安全なデバイス（例えば、非接触 IC カード 1 2 1）の記憶領域へ格納されてもよい。この場合、バリュー発行装置

1 4のバリュー発行部1 3 5で発行された電子バリューは、親機1 2の非接触ICカード1 2 1に転送される。例えば、バリュー発行装置1 4が、親機1 2-2から親機1 2-1に対してバリューを振り込む場合、バリュー発行装置1 4は、親機1 2-2からバリューを取得し、バリューを親機1 2-1に送信する。なお、

5 バリューの送受信は、バリューを暗号化して安全に行われる。

また、バリューは、バリュー発行装置1 4のバリュー記憶部1 4 0および親機1 2の安全なデバイスの両者の組み合わせによって記憶されてもよい。この組み合わせとして、バリュー発行装置1 4は、ユーザの電子バリューをバリュー記憶部1 4 0の中でそれぞれのユーザの口座として記憶し、その口座を管理しつつ、

10 必要な額だけをユーザのデバイス（例えば、非接触ICカード）へ移動させ財布のように利用させてもよい。

図1 6は、図1 5のバリュー発行装置1 4が振り込み通知書を親機1 2-1に送信する処理を説明するフローチャートである。この処理は、バリュー発行装置1 4が、親機1 2-2が図1 0のステップS 1 0 3で送信したバリュー移動要求を受信したとき開始される。なお、バリュー発行装置1 4は、認証装置1 3が発行した電子証明書を、既に証明書記憶部1 3 8に記憶しているものとする。

ステップS 1 6 1において、共通秘密鍵認証部1 3 3は、共通秘密鍵記憶部1 3 6から共通秘密鍵4 4と、秘密鍵記憶部1 3 7から秘密鍵4 3を読み出し、秘密鍵4 3を用いて、共通秘密鍵4 4を暗号化する。ステップS 1 6 1の処理後は、

20 ステップS 1 6 2に進み、共通秘密鍵認証部1 3 3は、その暗号化された共通秘密鍵4 4を親機1 2-2に送信し、ステップS 1 6 3に進む。即ち、共通秘密鍵認証部1 3 3は、暗号化された共通秘密鍵4 4を、データバス1 3 2を介して通信部1 3 1に供給し、通信部1 3 1は、その暗号化された共通秘密鍵4 4を親機1 2-2に送信する。

25 ステップS 1 6 3において、通信部1 3 1は、親機1 2-2から、図1 0のステップS 1 0 9で送信された暗号化された共通秘密鍵3 7を受信したかどうかを判定する。ステップS 1 6 3において、通信部1 3 1は、親機1 2-2から暗号

化された共通秘密鍵 3 7 を受信していないと判定した場合、ステップ S 1 6 4 に
進み、親機 1 2 - 2 から、図 1 0 のステップ S 1 1 0 で送信される、バリュー発
行装置 1 4 と親機 1 2 - 2 の関係が正当ではないことを示すエラー通知を受信し
たかどうかを判定する。ステップ S 1 6 8 において、通信部 1 3 1 は、エラー通
5 知を受信していないと判定した場合、ステップ S 1 6 3 に戻り、上述した処理を
繰り返す。

ステップ S 1 6 4 において、通信部 1 3 1 は、エラー通知を受信したと判定し
た場合、バリュー発行装置 1 4 と親機 1 2 - 2 の関係が正当ではないので、バリ
ュー移動の不許可を示すエラー通知を送信して処理を終了する。

10 一方、ステップ S 1 6 3 において、通信部 1 3 1 は、親機 1 2 - 2 から暗号化
された共通秘密鍵 3 7 を受信したと判定した場合、その暗号化された共通秘密鍵
3 7 を公開鍵認証部 1 3 4 に供給し、ステップ S 1 6 3 からステップ S 1 6 5 に
進む。ステップ S 1 6 5 において、公開鍵認証部 1 3 4 は、暗号化された共通秘
密鍵 3 7 を、秘密鍵記憶部 1 3 7 に記憶している秘密鍵 4 3 を用いて復号する。

15 ステップ S 1 6 5 の処理後は、ステップ S 1 6 6 に進み、公開鍵認証部 1 3 4
は、共通秘密鍵認証部 1 3 3 に、ステップ S 1 6 5 で復号した共通秘密鍵 3 7 を
供給し、共通秘密鍵認証部 1 3 3 は、復号した共通秘密鍵 3 7 と共通秘密鍵記憶
部 1 3 6 に記憶している共通秘密鍵 4 4 が等しいかどうかを判定する。

ステップ S 1 6 6 において、共通秘密鍵認証部 1 3 3 は、復号した共通秘密鍵
20 3 7 と共通秘密鍵 4 4 が等しいと判定した場合、親機 1 2 - 2 とバリュー発行装
置 1 4 の関係は正当であると認識して、ステップ S 1 6 6 からステップ S 1 6 7
に進む。即ち、この場合、親機 1 2 - 1 において公開鍵 4 1 を用いて暗号化され
た共通秘密鍵 3 7 が、バリュー発行装置 1 4 において、公開鍵 4 1 に対応する秘
密鍵 4 3 を用いて正常に復号され、共通秘密鍵 3 7 が得られているので、バリ
ュー発行装置 1 4 は、親機 1 2 - 2 とバリュー発行装置 1 4 が通信する間で改ざん
25 が行われていないと認識する。

さらに、バリュー発行装置 1 4 は、親機 1 2 - 2 が有する共通秘密鍵 3 7 とバ
リユー発行装置 1 4 が有する共通秘密鍵 4 4 が等しいので、親機 1 2 - 2 がバ
リユーを管理することを認められている相手であることを認識する。即ち、バリュ
ー発行装置 1 4 は、バリュー発行装置 1 4 の有する共通秘密鍵 4 4 と同一の秘密
5 鍵 3 7 を、親機 1 2 - 2 に備えられる安全なデバイス（非接触 I C カード 1 2
1）に配布し、親機 1 2 - 2 が共通秘密鍵 4 4 と等しい共通秘密鍵 3 7 を有する
ことを認識することによって、正しい親機 1 2 - 2 からのアクセスであることを
認識する。

ステップ S 1 6 7 において、バリュー発行部 1 3 5 は、親機 1 2 - 2 から親機
10 1 2 - 1 にバリューを移動する。即ち、バリュー発行部 1 3 5 は、バリュー記憶
部 1 4 0 に記憶された親機 1 2 - 2 の所定の対価に対応するバリューを削除し、
親機 1 2 - 1 のバリューに所定の対価に対応するバリューを追加し、これにより、
親機 1 2 - 2 のユーザの電子バリューが、そのユーザが移動端末装置 1 1 - 2 に
よってリソースを利用しようとしている親機 1 2 - 1 のユーザに対し、そのリソ
15 ースの利用に対する対価として振り込まれる。さらに、ステップ S 1 6 7 では、
バリュー発行部 1 3 5 は、バリューの移動完了を示す取引結果通知を生成する。

これにより、ユーザは、バリュー発行装置 1 4 を経由して、他のユーザとの間
で、電子バリューの授受を行うことができる。

ステップ S 1 6 7 の処理後は、ステップ S 1 6 8 に進み、公開鍵認証部 1 3 4
20 は、秘密鍵記憶部 1 3 7 に記憶された秘密鍵 4 3 を用いて、自らの正当性を証明
するために電子署名を暗号化する。そして、公開鍵認証部 1 3 4 は、その暗号化
した電子署名を付加した振込み通知書を作成する。この振込み通知書は、バリュ
ーの振込みを知らせるための振込み通知と、バリューの振込みの詳細が記載され
たレシートから構成されている。そして、公開鍵認証部 1 3 4 は、その振込み通
25 知書、証明書記憶部 1 3 8 に記憶された電子証明書、および電子バリューの移動
完了を示す取引結果通知を、バリューの振込先であるユーザの親機 1 2 - 1 に送
信して処理を終了する。

一方、ステップ S 1 6 6 において、共通秘密鍵認証部 1 3 3 は、ステップ S 1 6 5 で復号した共通秘密鍵と共通秘密鍵 4 4 が等しくないと判定した場合、親機 1 2-2 とバリュウ発行装置 1 4 の関係は正当ではないので、バリュウ移動の不許可を示すエラー通知を送信して処理を終了する。

5 図 1 7 は、図 1 の認証装置 1 3 の詳細構成例を示している。

認証装置 1 3 は、通信部 1 5 1、データベース 1 5 2、公開鍵認証部 1 5 3、秘密鍵記憶部 1 5 4、証明書記憶部 1 5 5、公開鍵記憶部 1 5 6、証明書記憶部 1 5 7、および証明書失効リスト記憶部 1 5 8 から構成されている。

10 通信部 1 5 1 は、インターネット 2 1 を介して、親機 1 2-1、親機 1 2-2、およびバリュウ発行装置 1 4 から送信された信号を受信するとともに、親機 1 2-1、親機 1 2-2、およびバリュウ発行装置 1 4 に信号を送信する。通信部 1 5 1 は、データベース 1 5 2 を介して、公開鍵認証部 1 5 3 と接続されている。

15 公開鍵認証部 1 5 3 は、公開鍵記憶部 1 5 6 に記憶された公開鍵と、一般公開用証明書記憶部 1 5 7 に記憶された一般公開用証明書を公開したり、電子証明書を発行する。また、公開鍵認証部 1 5 3 は、電子証明書が有効であるかどうかを判定する。

20 秘密鍵記憶部 1 5 4 には、秘密鍵 4 2 が記憶される。証明書記憶部 1 5 5 には、認証装置 1 3 の電子証明書が記憶される。公開鍵記憶部 1 5 6 には、親機 1 2-1 の秘密鍵 3 5 に対応する公開鍵 3 9、親機 1 2-2 の秘密鍵 3 8 に対応する公開鍵 4 0、およびバリュウ発行装置 1 4 の秘密鍵 4 3 に対応する公開鍵 4 1 が記憶される。

25 一般公開用証明書記憶部 1 5 7 には、公開鍵認証部 1 5 3 が発行した一般公開用の電子証明書が記憶され、この電子証明書が親機 1 2 やバリュウ発行装置 1 4 に提供される。証明書失効リスト記憶部 1 5 8 には、失効した電子証明書を示す証明書失効リストが記憶される。即ち、一般公開用証明書記憶部 1 5 7 に記憶された電子証明書が何らかの理由により失効したとき、その電子証明書が、その証明書失効リストにエントリされる。

図 18 は、図 17 の認証装置 13 が電子証明書の判定を行う処理を説明するフローチャートである。この処理は、親機 12 などから電子証明書の有効性の判定を要求する信号を受信したとき開始する。

5 ステップ S181 において、公開鍵認証部 153 は、証明書失効リスト記憶部 158 から、失効した電子証明書を示す証明書失効リストを読み出し、ステップ S182 に進む。ステップ S182 において、公開鍵認証部 153 は、親機 12 から受信した電子証明書の判定を要求する信号に基づいて、判定の対象となる電子証明書が失効しているかどうかを判定する。即ち、公開鍵認証部 153 は、ステップ S181 で読み出された証明書失効リストに、判定の対象となる電子証明
10 書があるかどうかを判定する。

ステップ S182 において、公開鍵認証部 153 は、判定の対象となる電子証明書が失効していると判定した場合、ステップ S183 に進み、データバス 152 を介して通信部 151 から、親機 12 に電子証明書の無効通知を送信して処理を終了する。

15 ステップ S182 において、公開鍵認証部 153 は、判定の対象となる電子証明書が失効していないと判定した場合、ステップ S184 に進み、データバス 152 を介して通信部 151 から、親機 12 に電子証明書の有効通知を送信して処理を終了する。

図 19 は、図 1 の通信システム 1 の全体の処理を説明するフローチャートである。即ち、図 19 のフローチャートは、移動端末装置 11-1 と移動端末装置 11-2 が親機 12-1 とのみ直接無線通信することができる場合に、その親機 12-1 に接続されたリソース機器 15-1 を利用するときの通信システム全体の処理を示している。

25 なお、図 19 では、移動端末装置 11-1、移動端末装置 11-2、親機 12-1、親機 12-1、認証装置 13、およびバリュウ発行装置 14 は、それぞれが通信する間で改ざんが行われず、正当な関係であるとする。

また、図 19 では、まず最初に、移動端末装置 11-1 がその本親機である親機 12-1 にリソースを要求し、その後、移動端末装置 11-2 が、無線通信で
きるが本親機でない親機 12-1 にリソースを要求するものとする。

ステップ S 231 において、移動端末装置 11-1 は、その本親機である親機
5 12-1 と双方向認証するために、共通秘密鍵 31 を暗号化して、親機 12-1
に送信する。

ステップ S 251 において、親機 12-1 は、移動端末装置 11-1 から暗号
化された共通秘密鍵 31 を受信する。ステップ S 252 において、親機 12-1
は、共通秘密鍵 33 を暗号化し、移動端末装置 11-1 に送信する。

10 ステップ S 232 において、移動端末装置 11-1 は、親機 12-1 から暗号
化された共通秘密鍵 33 を受信する。ステップ S 233 において、移動端末装置
11-1 は、その暗号化された共通秘密鍵 33 を復号し、復号した共通秘密鍵 3
3 を暗号化して、暗号化した共通秘密鍵 33 を親機 12-1 に送信する。

ステップ S 253 において、親機 12-1 は、暗号化された共通秘密鍵 33 を、
15 移動端末装置 11-1 から受信する。ステップ S 254 において、親機 12-1
は、暗号化された共通秘密鍵 33 を復号する。親機 12-1 は、復号した共通秘
密鍵 33 から、親機 12-1 と移動端末装置 11-1 の関係が正当であるかどう
かを判定する。この例では、親機 12-1 と移動端末装置 11-1 は正当な関係
であるので、親機 12-1 は、ステップ S 251 で移動端末装置 11-1 から受
20 信した暗号化された共通秘密鍵 31 を復号し、その復号した共通秘密鍵 31 を暗
号化して、移動端末装置 11-1 に送信する。

ステップ S 234 において、移動端末装置 11-1 は、親機 12-1 から暗号
化された共通秘密鍵 31 を受信し、その暗号化された共通秘密鍵 31 を復号する。
移動端末装置 11-1 は、復号した共通秘密鍵 31 から、親機 12-1 と移動端
25 末装置 11-1 の関係が正当であるかどうかを判定する。この例では、親機 12
-1 と移動端末装置 11-1 の関係は正当であるので、双方向認証を完了し、ス

ステップS 2 3 5において、移動端末装置 1 1-1 は、リソースを要求する信号を親機 1 2-1 に送信する。

即ち、移動端末装置 1 1-1 は、その本親機である親機 1 2-1 と双方向認証することにより、移動端末装置 1 1-1 を使用するユーザが正しいユーザである

5 ことを、通信システム 1 のユーザに保証する。

ステップS 2 5 5において、親機 1 2-1 は、移動端末装置 1 1-1 からリソースを要求する信号を受信する。ステップS 2 5 6において、親機 1 2-1 は、リソースを要求する信号に基づいて、要求対象となるリソース機器 1 5-1 にリソースを要求する信号を送信する。

10 ステップS 2 9 1において、リソース機器 1 5-1 は、親機 1 2-1 からリソースを要求する信号を受信する。ステップS 2 9 2において、リソース機器 1 5-1 は、リソースを要求する信号に基づいて、要求対象となるリソースを親機 1 2-1 を介して、移動端末装置 1 1-1 に送信する。

15 ステップS 2 3 6において、移動端末装置 1 1-1 は、リソース機器 1 5-1 から親機 1 2-1 を介して、リソースを受信し、これにより、リソース機器 1 5-1 を利用することが可能な状態となる。

一方、移動端末装置 1 1-2 は、ステップS 2 0 1において、リソース情報を取得するために、その本親機でない親機 1 2-1 にデバイス探索を要求する信号を送信する。

20 ステップS 2 5 7において、親機 1 2-1 は、移動端末装置 1 1-2 からデバイス探索を要求する信号を受信し、デバイス探索要求を許可するかどうかを判定する。図 1 9 では、ステップS 2 5 8において、親機 1 2-1 は、デバイス探索を許可し、デバイス探索を許可する信号を、移動端末装置 1 1-2 に送信する。

25 ステップS 2 0 2において、移動端末装置 1 1-2 は、親機 1 2-1 からデバイス探索を許可する信号を受信する。ステップS 2 0 3において、移動端末装置 1 1-2 は、親機 1 2-1 が取得できるリソースの情報（親機 1 2-1 が、移動

端末装置 11-2 に提供することができるリソースの情報) を要求する信号を、親機 12-1 に送信する。

ステップ S259 において、親機 12-1 は、移動端末装置 11-2 からリソースの情報を要求する信号を受信する。ステップ S260 において、親機 12-

5 1 は、リソース情報を移動端末装置 11-2 に送信する。

ステップ S204 において、移動端末装置 11-2 は、親機 12-1 からリソース情報を受信する。ステップ S205 において、移動端末装置 11-2 は、親機 12-2 と双方向認証をするため、共通秘密鍵 32 を暗号化し、その暗号化した共通秘密鍵 32 を親機 12-2 に送信する。

10 ステップ S311 において、親機 12-2 は、移動端末装置 11-2 から、暗号化された共通秘密鍵 32 を受信する。ステップ S312 において、親機 12-2 は、共通秘密鍵 36 を暗号化し、暗号化した共通秘密鍵 36 を移動端末装置 11-2 に送信する。

ステップ S206 において、移動端末装置 11-2 は、親機 12-2 から暗号化した共通秘密鍵 36 を受信し、暗号化した共通秘密鍵 36 を復号する。移動端末装置 11-2 は、復号した共通秘密鍵 36 から、移動端末装置 11-2 と親機 12-2 の関係が正当であるかどうかを判定する。この例の場合、移動端末装置 11-2 と親機 12-2 の関係は正当であるので、ステップ S207 において、移動端末装置 11-2 は、復号した共通秘密鍵 36 を暗号化し、暗号化した共通秘密鍵 36 を親機 12-2 に送信する。

ステップ S313 において、親機 12-2 は、移動端末装置 11-2 から暗号化した共通秘密鍵 36 を受信し、その暗号化した共通秘密鍵 36 を復号する。親機 12-2 は、復号した共通秘密鍵 36 から、親機 12-2 と移動端末装置 11-2 の関係は正当であるかどうかを判定する。この例の場合、親機 12-2 と移動端末装置 11-2 の関係は正当であるので、ステップ S314 において、親機 12-2 は、ステップ S311 で移動端末装置 11-2 から受信した暗号化さ

れた共通秘密鍵 3 2 を復号し、復号した共通秘密鍵 3 2 を暗号化する。親機 1 2 - 2 は、その暗号化した共通秘密鍵 3 2 を移動端末装置 1 1 - 2 に送信する。

ステップ S 2 0 8 において、移動端末装置 1 1 - 2 は、親機 1 2 - 2 から暗号化された共通秘密鍵 3 2 を受信し、その暗号化された共通秘密鍵 3 2 を復号する。

- 5 移動端末装置 1 1 - 2 は、復号した共通秘密鍵 3 2 から、移動端末装置 1 1 - 2 と親機 1 2 - 2 の関係が正当であるかどうかを判定する。この例では、移動端末装置 1 1 - 2 と親機 1 2 - 2 の関係が正当であるので、双方向認証を完了し、ステップ S 2 0 9 において、移動端末装置 1 1 - 2 は、リソースを要求する信号を親機 1 2 - 2 に送信する。

- 10 ステップ S 3 1 5 において、親機 1 2 - 2 は、移動端末装置 1 1 - 2 から、リソースを要求する信号を受信する。ステップ S 3 1 6 において、親機 1 2 - 2 は、親機 1 2 - 1 にリソース情報の識別子と利用方法を明記した利用権発行要求と電子証明書を、親機 1 2 - 1 に送信する。

- 15 ステップ S 2 6 1 において、親機 1 2 - 1 は、親機 1 2 - 2 から利用権発行要求と電子証明書を受信する。ステップ S 2 6 2 において、親機 1 2 - 1 は、その電子証明書が有効であるかどうかの判定要求を認証装置 1 3 に送信する。

- 20 ステップ S 3 6 1 において、認証装置 1 3 は、親機 1 2 - 1 から電子証明書の判定要求を受信し、その電子証明書が有効であるかどうかを判定する。なお、ここでは、電子証明書は有効であるものとし、ステップ S 3 6 2 において、認証装置 1 3 は、親機 1 2 - 1 に対象の電子証明書が有効であることを示す信号を送信する。

- 25 ステップ S 2 6 3 において、親機 1 2 - 1 は、認証装置 1 3 から電子証明書が有効であることを示す信号を受信する。ステップ S 2 6 4 において、親機 1 2 - 1 は、リソースの利用を許可するための対価を記載したリソース利用条件文と電子証明書を、親機 1 2 - 2 に送信する。

ステップS 3 1 7において、親機1 2-2は、親機1 2-1からリソース利用条件文と電子証明書を受信する。ステップS 3 1 8において、親機1 2-2は、バリュー発行装置1 4にバリュー移動要求を送信する。

5 ステップS 3 4 1において、バリュー発行装置1 4は、親機1 2-2からバリュー移動要求を受信する。ステップS 3 4 2において、バリュー発行装置1 4は、親機1 2-2と双方向認証するため、共通秘密鍵4 4を暗号化して、暗号化した共通秘密鍵4 4を親機1 2-2に送信する。

10 ステップS 3 2 0において、親機1 2-2は、バリュー発行装置1 4から、暗号化された共通秘密鍵4 4を受信し、その暗号化された共通秘密鍵4 4を復号する。親機1 2-2は、復号した共通秘密鍵4 4から、親機1 2-2とバリュー発行装置1 4の関係が正当であるかどうかを判定する。この例の場合、親機1 2-2とバリュー発行装置1 4の関係は正当であるので、ステップS 3 2 0において、親機1 2-2は、共通秘密鍵3 7を暗号化し、暗号化した共通秘密鍵3 7をバリュー発行装置1 4に送信する。

15 ステップS 3 4 3において、バリュー発行装置1 4は、親機1 2-2から暗号化された共通秘密鍵3 7を受信し、その暗号化された共通秘密鍵3 7を復号する。バリュー発行装置1 4は、復号した共通秘密鍵3 7から、バリュー発行装置1 4と親機1 2-2の関係が正当であるかどうかを判定する。この例の場合、バリュー発行装置1 4と親機1 2-2の関係は正当であるので、ステップS 3 4 4において、バリュー発行装置1 4は、ステップS 3 4 1で受信したバリュー移動要求に応じてバリューを移動し、即ち、ここでは、親機1 2-1のユーザから親機1 2-1のユーザにバリューを移動し、バリューが移動されたことを示す振込み通知と電子証明書を、親機1 2-1に送信する。

25 ステップS 2 6 5において、親機1 2-1は、バリュー発行装置1 4から、振込み通知書と電子証明書を受信する。ステップS 2 6 6において、親機1 2-1は、その電子証明書が有効であるかどうかの判定を要求する信号を認証装置1 3に送信する。

ステップS 3 6 3において、認証装置1 3は、親機1 2-1から、電子証明書の判定を要求する信号を受信し、その電子証明書が有効であるかどうかを判定する。この例の場合、親機1 2-2の電子証明書は有効であるので、ステップS 3 6 4において、認証装置1 3は、親機1 2-1に対象の電子証明書が有効であることを示す信号を送信する。

ステップS 2 6 7において、親機1 2-1は、認証装置1 3から電子証明書が有効であることを示す信号を受信する。ステップS 2 6 8において、親機1 2-1は、リソースを利用する権利を記載した権利文を発行し、その権利文と電子証明書を親機1 2-2に送信する。

10 ステップS 3 2 1において、親機1 2-2は、親機1 2-1から送信されてくる権利文と電子証明書を受信する。ステップS 3 2 2において、親機1 2-2は、その電子証明書が有効であるかどうかの判定を要求する信号を認証装置1 3に送信する。

15 ステップS 3 6 5において、認証装置1 3は、親機1 2-2から、電子証明書の判定を要求する信号を受信し、その電子証明書が有効であるかどうかを判定する。この例の場合、親機1 2-1の電子証明書は有効であるので、ステップS 3 6 6において、認証装置1 3は、親機1 2-2に対象の電子証明書が有効であることを示す信号を送信する。

20 ステップS 3 2 3において、親機1 2-2は、認証装置1 3から電子証明書が有効であることを示す信号を受信する。ステップS 3 2 4において、親機1 2-2は、ステップS 3 2 1で、親機1 2-1から受信した権利文を、移動端末装置1 1-2に送信する。

25 ステップS 2 1 0において、移動端末装置1 1-2は、親機1 2-1から権利文を受信する。ステップS 2 1 1において、移動端末装置1 1-2は、その権利文とリソースを要求する信号を、親機1 2-1に送信する。

ステップS 2 6 9において、親機1 2-1は、移動端末装置1 1-2から、権利文とリソースを要求する信号を受信する。ステップS 2 7 0において、親機1 2-1は、リソース機器1 5-1にリソースを要求する信号を送信する。

5 ステップS 2 9 3において、リソース機器1 5-1は、親機1 2-1からリソースを要求する信号を受信する。ステップS 2 9 4において、リソース機器1 5-1は、親機1 2-1から要求されたリソースを親機1 2-1を介して、移動端末装置1 1-2に送信する。

ステップS 2 1 2において、リソース機器1 5-1から、リソースを受信する。

10 以上により、移動端末装置1 1-2は、親機1 2-1から権利文を取得することにより、親機1 2-1に接続されたリソース機器1 5-1を利用できる環境を得ることができる。

以上のように、通信システム1では、バリュー発行装置1 4は、バリューの管理をする親機1 2に対して共通秘密鍵4 4と同一の秘密鍵3 4や3 7を送信し、親機1 2の非接触ICカード1 2 1に記憶させる。親機1 2は、個人情報に格納するユーザに、親機1 2と通信可能にするための共通秘密鍵を格納した非接触ICカード7 1を発行する。これにより、ユーザは、非接触ICカード7 1の情報を移動端末装置1 1に読み込ませるだけで、本親機である親機1 2と通信をし、バリューの移動をすることができる。そして、ユーザは、上述した一連の処理を、例えば、非接触ICカード7 1を移動端末装置1 1に、ワンタッチすることで行
20 わせることができ、この場合、利便性の高い付加価値を提供することができる。

さらに、認証情報やそれに伴うユーザの個人情報を管理する本親機となる親機1 2を、例えばユーザ宅のホームサーバという形で、移動端末装置1 1とは別に設けたので、ユーザと移動端末装置1 1とは依存関係がなく、リソースの利用時にのみユーザの認証を行えば済む。また、ユーザは、個人情報をバリュー発行装置に管理させることなく、自らの所有する親機1 2に格納し、バリューの決済情報だけを親機1 2とバリュー発行装置1 4との間でやりとりするだけで済む。さらに、ユーザが移動する場合においても、ユーザは、移動した空間にある機器

(リソース) を、匿名のままユーザの嗜好に合わせた操作性で操作することができる。

また、図 1 の通信システム 1 によれば、ユーザが、移動した空間にある移動端末装置 11-2 を操作することにより、そのユーザが個人情報管理する親機

- 5 (本親機) 12-2 が、バリュー発行装置 14 の仲介の下、他人の親機 12-1 に電子バリューを支払って、その親機 12-1 のリソースの利用権を入手し、その利用権を、移動端末装置 11-2 が受け取って、親機 12-1 に提示することで移動端末装置 11-2 のユーザは、他人の親機 12-1 のリソースを、匿名のまま利用することができる。即ち、バリュー発行装置 14 は、移動端末装置 11-2 のユーザの親機 12-2 から他人の親機 12-1 に対しての電子バリューの振込みを仲介するだけであり、ユーザの個人情報の管理は、親機 12 で行われる。従って、電子バリューの決済の場と、個人情報の管理の場とが完全に分離されているといえることができる。なお、移動端末装置 11-2 からバリュー発行装置 14 にアクセスし、電子バリューを、リソースを利用しようとする親機 12-1 に
- 10 振込み、移動端末装置 11-2 から親機 12-1 のリソースを利用することも可能である。但し、この場合、親機 12-1 に対する、移動端末装置 11-2 のユーザの匿名性は確保されるが、移動端末装置 11-2 のユーザの個人情報の管理は、移動端末装置 11-2 がアクセスするバリュー発行装置 14 で行われることになる。

- 20 さらに、移動端末装置 11-2 は、リソースを利用する親機 12-1 を介して、本親機である親機 12-2 にアクセスして、そのリソースの利用権を取得するので、利用したいリソースに近い位置で、その利用権を得ることができる。

- ここで、移動端末装置 11 としては、例えば、PDA(Personal Digital Assistant)や、携帯用コンピュータ、携帯電話機、腕時計、デジタルスチルカメラ、
- 25 デジタルビデオカメラなどの携帯性に優れた装置を採用することが可能である。

また、出先のユーザが移動端末装置 11 から利用するリソースとしては、例えば、「装置」や、「情報」、「情報に対するライセンス」などがある。

リソースとしての「装置」には、例えば、無線アクセスポイントや、テレビジョン受像機、電話機などが含まれる。リソースとして「装置」を利用するケースとしては、例えば、出先のユーザが、移動端末装置 1 1 から、他人の無線アクセスポイントを利用してインターネットに接続する場合がある。

5 また、リソースとしての「情報」には、いわゆるホームサーバやチャンネルサーバなどで構成される親機 1 2 - 1 が管理するコンテンツその他の情報などが含まれる。リソースとして「情報」を利用するケースとしては、例えば、出先のユーザが、親機 1 2 - 1 としてのチャンネルサーバに蓄えられたコンテンツを視聴する場合がある。

10 さらに、リソースとしての「情報に対するライセンス」には、情報が暗号化されている場合に、その暗号化を解くための鍵などが含まれる。リソースとして「情報に対するライセンス」を利用するケースとしては、例えば、携帯端末装置 1 1 に、ネットワーク経由でダウンロードした、暗号化されたコンテンツを視聴する場合に、そのコンテンツを視聴するためのライセンスとしての暗号鍵を取得
15 するときなどがある。

なお、上述した一連の処理では、移動端末装置 1 1 - 1 と移動端末装置 1 1 - 2 のユーザは異なっていたが、同一ユーザの親機や移動端末装置間でも同様に電子バリューの移動をすることができる。

上述した実施の形態に関し、具体例を挙げてさらに説明を加える。

20 図 2 0 は、ユーザ B がユーザ A の家で、ユーザ A の P C (パーソナルコンピュータ) を借り、その対価を支払う例を説明するための図であり、そのような場合におけるシステムの構成例を示している。移動端末装置 2 0 1 - 1 は、ユーザ A が所持する装置であり、移動端末装置 2 0 1 - 2 は、ユーザ B が所持する装置である。移動端末装置 2 0 1 - 1, 2 0 1 - 2 は、それぞれ携帯電話や、携帯可能な C D プレーヤなどである。
25

移動端末装置 201-1 には、ユーザ A のホームサーバ 202-1 のアドレスが登録され、移動端末装置 201-2 には、ユーザ B のホームサーバ 202-2 のアドレスが登録されている。

ユーザ A が管理するホームサーバ 202-1 は、同じくユーザ A が管理している PC 203 や TV (テレビジョン受像機) 204 を管理する。この PC 203 や TV 204 は、家庭内ネットワークを介してホームサーバ 202-1 と接続されているリソースである。また、ホームサーバ 202-1 は、ユーザ A の個人情報も保管している。

同様に、ユーザ B が管理するホームサーバ 202-2 は、ユーザ B が管理するリソースを管理すると共に、ユーザ B の個人情報も保管する。ホームサーバ 202-1 やホームサーバ 202-2 は、それぞれ無線により直接的に、または、アクセスポイント (図 20 においては不図示) を介して他のホームサーバと通信することができるように構成されている。

また、携帯端末装置 201-1, 201-2 は、接続したホームサーバ 202-1, 202-2 を介し、そしてインターネット 205 を経由し、他のホームサーバなどと通信することができるように構成されている。

インターネット 205 には、認証装置 206 も接続されている。認証装置 206 は、PKI 処理のための証明書を発行する機関が管理する装置であり、証明書の管理を行うための装置である。インターネット 205 には、バリュ発行装置 207 も接続されている。バリュ発行装置 207 は、各ユーザのバリュの交換を仲介する装置 (対価の支払いに係わる処理を実行する装置) である。

ここで、図 20 に示したシステムと図 1 に示したシステムとの対応関係を記載しておく。移動端末装置 201-1 は、移動端末装置 11-1 であり、移動端末装置 201-2 は、移動端末装置 11-2 である。ホームサーバ 202-1 は、親機 12-1 であり、ホームサーバ 202-2 は、親機 12-2 である。PC 203 は、リソース機器 16-2 であり、TV 204 は、リソース機器 15-2 である。

インターネット 205 は、インターネット 21 であり、認証装置 206 は、認証装置 13 である。バリュー発行装置 207 は、バリュー発行装置 14 である。このように、図 20 は、図 1 と対応関係があり、図 1 およびそれ以降の図を参照して説明した事項は、図 20 に示したシステムに関する事項として適用できるため、既に説明した部分については、適宜説明を省略する。

次に、図 21 のフローチャートを参照し、ユーザ B が移動端末装置 201-2 を保持している状態でユーザ A 宅に行き、ユーザ A 宅に設置され、ユーザ A により管理されている PC 203 を使用するとき、図 20 に示したシステムで行われる処理について説明する。なお、以下の説明においては、認証局（認証装置 206）で PKI により行われる、各ユーザのアクセスの信頼性を確認する手順については、既に説明した事項と重なるため省略する。

まず、移動端末装置の初期化に係わる処理が実行される。移動端末装置の初期化に係わる処理は、ここでは、移動端末装置 201-2 とホームサーバ 202-2 との間で行われる。まずステップ S401 において、ユーザ B が保持する移動端末装置 201-2 は、ホームサーバ 202-2 にアクセスする。

ステップ S471 において移動端末装置 201-2 からのアクセスを受けたホームサーバ 202-2 は、ステップ S472 において、自己が管理しているユーザ B の個人情報の一部を送信する。送信された個人情報は、ステップ S402 において、移動端末装置 201-2 に受信され、保持される。

移動端末装置 201-2 には、ホームサーバ 202-2 のアドレスが登録されているため、ホームサーバ 202-2 にアクセスすることが可能とされている。また、移動端末装置 201-2 は、ユーザ B が登録されており、ユーザ B しか使うことができないように構成されている。例えば、ユーザ B の指紋が登録されており、指紋認証が正常に行われないう限り、移動端末装置 201-2 は起動されないように構成されている。

そして、指紋認証などが用いられた認証処理が正常に行われた後（この場合、ユーザ B であると確認がとれた後）、移動端末装置 201-2 は、使用可能な状

態とされる。使用可能な状態とされた後、ホームサーバ 202-2 とアクセス可能であれば、上述したような処理が、移動端末装置 201-2 とホームサーバ 202-2 との間で実行される。

移動端末装置 201-2 は、ユーザ B の個人情報を保持した後の時点で、定期的にデバイス探索要求を発信している（ステップ S 403）。その定期的に発信されているデバイス探索要求を、ステップ S 421 の処理として受信したホームサーバ 202-1 は、ステップ S 422 において、自己のアドレス、デバイス探索要求を発信してきた端末（この場合、移動端末装置 201-2）に一時的に与える ID、および、移動端末装置 201-2 がインターネット 205 を介して他の装置とデータの授受を行えるようにするために必要となる情報（例えば、デフォルトルータのアドレスなど）を、移動端末装置 201-2 に通知する。

このようなホームサーバ 202-1 からのデータは、ステップ S 404 において、移動端末装置 201-2 に受信され、記憶される。ステップ S 405 において、移動端末装置 201-2 は、ホームサーバ 202-2 に対してリソース要求を出す。移動端末装置 201-2 は、先程の処理で、ホームサーバ 202-2 のアドレスを取得し記憶しているため、ホームサーバ 202-2 と通信することができる状態とされている。なお、この通信の際、必要に応じ、ホームサーバ 202-1 から与えられた ID も用いられる。

ステップ S 423 において、ホームサーバ 202-1 は、リソース要求を受信すると、ステップ S 424 の処理として、自己の管理するリソースに関する情報を、移動端末装置 201-2 に対して通知する。リソース情報として、ホームサーバ 202-1 から移動端末装置 201-2 に対して通知される情報について説明する。

リソース情報は、リソースの名前、設置場所、現在使用中であるか否かを表す情報、使用する際に必要となる対価、移動端末装置から操作できる操作のリストなどを含む情報である。例えば、図 20 を参照するに、ホームサーバ 202-1 には、PC 203 が接続されている。PC 203 に関するリソース情報としては、

PC203という名称であり、例えば、居間に設置され、現在使用中ではなく、対価として例えば100円を必要とし、移動端末装置201-2から操作できる操作のリストを含む情報である。

同様のリソース情報が、ホームサーバ202-1に接続されているTV204
5 に関しても作成され、PC203のリソース情報と合わせて、移動端末装置201-2に対して通知される。

このようなリソース情報を、ステップS406の処理として受信した移動端末装置201-2は、そのリソース情報を記憶する。

このようにして、リソース情報を取得した移動端末装置201-2は、次に、
10 リソースの選択に係わる処理を実行する。

まず前提として、移動端末装置201-2は、取得したリソース情報を基に、ユーザにリソースに関する情報を提示する。提示の仕方は、どのようなものでも良いが、例えば、移動端末装置201-2は、図2に示すような構成を有し、表示部64を有していれば、その表示部64を用いて提示が行われるように構成する。具体的には、まず表示部64に、リソースの一覧（この場合、例えば、PC
15 203とTV204が列記されたものである）が表示される。その一覧を参照しユーザBが、使用したいリソース（機器）を選択すると、その選択された機器に関する詳細な情報に、表示部64の表示が切り換えられる。

このようにして、ホームサーバ202-1から詳細情報まで含まれるリソース
20 情報が通知され、段階的にユーザに提示されるようにしても良い。

他のリソース情報の提示の仕方としては、リソース（例えば、PC203）と直接的に近接通信を行うことにより、そのリソースの詳細な情報が取得されるようにしても良い。例えば、まず、ステップS407において、移動端末装置201-2からPC203に対して、近接通信によりリソース情報の要求が出される。

25 そのような要求をステップS451において受信したPC203は、ステップS452において、自己の詳細な情報（例えば、使用するのに必要とされる金額など）を移動端末装置201-2に対して通知する。そのような通知を、ステッ

プ S 4 0 8 において受信した移動端末装置 2 0 1 - 2 は、その受信した情報を、ユーザ B に対して提示する。

いずれの手順により、リソース情報が移動端末装置 2 0 1 - 2 に対して通知されるようにしても良いが、結果としてユーザ B は、リソース情報を参照し、使用
5 したい機器を選択する。ここでは、ユーザ B は、P C 2 0 3 を使用したい機器として選択したとして説明を続ける。

ユーザ B が、使用したい機器として P C 2 0 3 を選択すると、移動端末装置 2 0 1 - 2 の表示部 6 4 には、“1 時間 1 0 0 円で使用しますか？”といったようなメッセージが表示される。これは、ユーザ A が所有する P C 2 0 3 を使用する
10 ことにより、その対価を支払わなくてはならないといったようなことをユーザ B に認識させるためのものである。ユーザ B は、そのようなメッセージを確認し、対価を支払って P C 2 0 3 を使用する場合、所定の操作、例えば、表示部 6 4 に表示された“Y E S”といったようなボタン（不図示）を操作する。

そのような操作が行われた場合、移動端末装置 2 0 1 - 2 は、ステップ S 4 0
15 9 において、ホームサーバ 2 0 2 - 2 に対して、使用したいリソース（この場合、P C 2 0 3）と、そのリソースを管理するホームサーバ（この場合、ホームサーバ 2 0 2 - 1）のアドレスを通知する。このような通知を、ステップ S 4 7 3 の処理として受信したホームサーバ 2 0 2 - 2 は、ステップ S 4 7 4 において、ホームサーバ 2 0 2 - 1 に対して、当該リソースの使用を要求する旨と、使用条件
20 （この場合、例えば、1 時間使用するという条件）を通知する。

このような通知を、ステップ S 4 2 5 の処理として受信したホームサーバ 2 0 2 - 1 は、ステップ S 4 2 6 において、自己に登録された機器（リソース）情報から、通知された使用条件（この場合、1 時間使用するという条件）を満たすために、ユーザ B が支払うべき対価（この場合、1 時間 × 1 0 0 円 = 1 0 0 円とい
25 う計算がなされる）を算出し、その算出結果を、トランザクション番号と共に、ホームサーバ 2 0 2 - 2 に対して通知する。

ステップS 4 7 5において、ホームサーバ2 0 2-1からの通知を受信したホームサーバ2 0 2-2は、ステップS 4 7 6において、バリュー発行装置2 0 7に対して、トランザクション番号と共に、ホームサーバ2 0 2-1宛にバリューの振り込み要求を行う。バリュー発行装置2 0 7は、ステップS 4 9 1において、
5 ホームサーバ2 0 2-2からの通知を受信すると、ホームサーバ2 0 2-1との間で、バリューの振り込みの処理が実行される（ステップS 4 9 2、ステップS 4 2 7）。

またバリュー発行装置2 0 7は、ホームサーバ2 0 2-2との間で、バリューの減額処理を実行する（ステップS 4 9 3、ステップS 4 7 7）。このようにして、バリュー発行装置2 0 7は、ホームサーバ2 0 2-1に対してバリューの振り込みの処理を実行し、その振り込みされるバリューを、ホームサーバ2 0 2-2から減額するという処理を実行する。
10

バリューの振り込み、減額の処理がそれぞれ正常に行われると、バリュー発行装置2 0 7は、ステップS 4 9 4において、ホームサーバ2 0 2-1に対して、
15 トランザクションが正常に終了されたことを、トランザクション番号と共に通知する。

ホームサーバ2 0 2-1は、このような通知をバリュー発行装置2 0 7から、ステップS 4 2 8において受信すると、ステップS 4 2 9において、トランザクション番号から、使用を許可する（使用を要求されていた）機器、その使用条件、
20 および、使用権を、ホームサーバ2 0 2-2に対して発行する。同様の情報を、ステップS 4 3 0において、ホームサーバ2 0 2-1は、PC 2 0 3に対しても発行する。

ステップ4 7 8において、ホームサーバ2 0 2-1により発行された使用権などを受信したホームサーバ2 0 2-2は、ステップS 4 7 9において、移動端末
25 装置2 0 1-2に対して、使用権を渡す。

ステップS 4 1 0において、ホームサーバ2 0 2-2から使用権を受信した移動端末装置2 0 1-2は、ステップS 4 1 1において、PC 2 0 3に対して、使

用権を提示する。この提示は、ホームサーバ202-1を介して行われても良いし、直接的に近距離無線通信などが用いられて行われるようにしても良い。使用権を提示されたPC207は、ステップS455において、まず、ホームサーバ202-1から渡された使用権と、移動端末装置201-2から提示された使用権が一致するか否かを判断する。

使用権が一致すると判断された場合、ステップS455において、PC207は、移動端末装置201-2に対してアクセス許可を通知する。なお、使用権が一致しないと判断された場合、PC207は、アクセス許可を通知しない（アクセス許可をしないということを通知するようにしても良い）。

- 10 PC207は、アクセス許可を通知することにより、また、移動端末装置201-2は、アクセス許可を通知されることにより、互いにデータの授受が行える状態とされる。すなわち、PC207は、移動端末装置201-2からの操作指示を受け入れる状態とされる。このように、移動端末装置201-2で、PC207を操作できる状態とされた場合、移動端末装置201-2の所有者であるユーザBの嗜好が反映された形でPC207を操作できるようにするための情報が、
- 15 移動端末装置201-2からPC207に対して通知される。

- すなわち、ステップS413において、移動端末装置201-2は、PC207に対して、自己が管理しているユーザBの嗜好情報を通知する。PC207は、そのような嗜好情報を受信すると、その嗜好情報に基づき、ユーザB用にカスタマイズされた環境を構築する。例えば、嗜好情報として、ユーザBがいつも使用
- 20 しているログイン画面に関する情報が通知された場合、その画面がログイン時にPC207のディスプレイ（不図示）上に表示される。

このように、本発明を適用することにより、他のユーザが管理する装置を対価を支払って使用することが可能となる。

- 25 なお、本明細書において、フローチャートに記載された処理は、ステップとして記載された順序に従って時系列的に行われる処理はもちろん、必ずしも時系列

的に処理されなくとも、並列的あるいは個別に実行される処理をも含むものである。

また、本明細書において、システムとは、複数の装置により構成される装置全体を表わすものである。

5

産業上の利用可能性

本発明によれば、特に、ユーザが移動する場合においても、移動した空間にある機器を、匿名のまま操作させることができる。また、そのとき発生する対価の支払いを自動的に行うことができる。さらに、利便性がよく、安全な通信をする

10 ことができる。

請求の範囲

1. ユーザにより操作される端末と、

リソースを提供する第1の親機と、

前記ユーザの個人情報を記憶する第2の親機と、

5 電子バリューを管理するバリュー装置と

を備える情報処理システムにおいて、

前記端末は、

前記第1の親機が提供するリソースを要求する信号を、前記第2の親機に送信するリソース要求信号送信手段と、

10 前記第1の親機が提供するリソースを利用する利用権を、前記第2の親機から取得する第1の利用権取得手段と

を有し、

前記利用権を、前記第1の親機に提示して、前記第1の親機が提供するリソースを利用し、

15 前記第1の親機は、

前記リソースの提供に対する対価としての電子バリューが、前記第2の親機から前記第1の親機に振り込まれたことの振込み通知を、前記バリュー装置から受信する振込み通知受信手段と、

前記振込み通知に応じて、前記第2の親機に対して、前記利用権を発行する

20 利用権発行手段と

を有し、

前記端末が、前記利用権を提示した場合に、自身が有するリソースの利用を許可し、

前記第2の親機は、

25 前記端末装置から送信されてくる、前記リソースを要求する信号に応じて、前記第1の親機への前記電子バリューの振込みを、前記バリュー装置に要求する電子バリュー振込み要求手段と、

前記電子バリューの振込みに応じて、前記第 1 の親機が発行する前記利用権を取得する第 2 の利用権取得手段と、

前記第 2 の利用権取得手段において取得された前記利用権を、前記端末に提供する利用権提供手段と

5 を有し、

前記バリュー装置は、

前記第 2 の親機からの要求に応じて、前記第 1 の親機に前記電子バリューを振り込む電子バリュー振込み手段と、

10 前記第 1 の親機への前記電子バリューの振込み通知を、前記第 1 の親機に送信する振込み通知送信手段と

を有する

ことを特徴とする情報処理システム。

2. ユーザにより操作される情報処理装置において、

15 リソースを提供する第 1 の親機が提供するリソースを要求する信号を、前記ユーザの個人情報を記憶する第 2 の親機に送信するリソース要求信号送信手段と、

前記第 1 の親機が提供するリソースを利用する利用権を、前記第 2 の親機から取得する利用権取得手段と

を備え、

20 前記利用権を、前記第 1 の親機に提示して、前記第 1 の親機が提供するリソースを利用する

ことを特徴とする情報処理装置。

3. 前記第 2 の親機との間で、前記ユーザが前記第 2 の親機が記憶している個人情報に対応する正当なユーザであることの認証を行う認証手段を

さらに備えることを特徴とする請求の範囲第 2 項に記載の情報処理装置。

25 4. 前記リソース要求信号送信手段と前記利用権取得手段は、前記第 1 の親機を介して、前記第 2 の親機とやりとりする

ことを特徴とする請求の範囲第 2 項に記載の情報処理装置。

5. 前記リソース要求信号送信手段と前記利用権取得手段は、前記第2の親機との間で、データを暗号化してやりとりする

ことを特徴とする請求の範囲第2項に記載の情報処理装置。

6. 前記リソースは、装置、情報、または情報に対するライセンスである

5 ことを特徴とする請求の範囲第2項に記載の情報処理装置。

7. ユーザにより操作される情報処理装置の情報処理方法において、

リソースを提供する第1の親機が提供するリソースを要求する信号を、前記ユーザの個人情報を記憶する第2の親機に送信するリソース要求信号送信ステップと、

10 前記第1の親機が提供するリソースを利用する利用権を、前記第2の親機から取得する利用権取得ステップと

を含み、

前記利用権を、前記第1の親機に提示して、前記第1の親機が提供するリソースを利用する

15 ことを特徴とする情報処理方法。

8. ユーザにより操作される情報処理装置に実行させるプログラムであって、

リソースを提供する第1の親機が提供するリソースを要求する信号を、前記ユーザの個人情報を記憶する第2の親機に送信するリソース要求信号送信ステップと、

20 前記第1の親機が提供するリソースを利用する利用権を、前記第2の親機から取得する利用権取得ステップと

を含み、

前記利用権を、前記第1の親機に提示して、前記第1の親機が提供するリソースを利用する

25 ことを特徴とするプログラム。

9. ユーザにより操作される端末に、自身が有するリソースを提供する情報処理装置において、

前記リソースの提供に対する対価としての電子バリューが、前記ユーザの個人情報情報を記憶する親機から振り込まれたことの振込み通知を、電子バリューを管理するバリュー装置から受信する振込み通知受信手段と、

前記振込み通知に応じて、前記親機に対して、自身が有するリソースを利用す

5 る利用権を発行する利用権発行手段と

を備え、

前記端末が、前記親機から取得した前記利用権を提示した場合に、自身が有するリソースの利用を許可する

ことを特徴とする情報処理装置。

10 10. 前記バリュー装置との間で、前記電子バリューを扱う正当な装置であることの認証を行う認証手段をさらに備える

ことを特徴とする請求の範囲第9項に記載の情報処理装置。

11. 前記振込み通知が正当であることの認証を行う認証手段をさらに備える

15 ことを特徴とする請求の範囲第9項に記載の情報処理装置。

12. 前記リソースは、装置、情報、または情報に対するライセンスであることを特徴とする請求の範囲第9項に記載の情報処理装置。

13. ユーザにより操作される端末に、自身が有するリソースを提供する情報処理装置の情報処理方法において、

20 前記リソースの提供に対する対価としての電子バリューが、前記ユーザの個人情報情報を記憶する親機から振り込まれたことの振込み通知を、電子バリューを管理するバリュー装置から受信する振込み通知受信ステップと、

前記振込み通知に応じて、前記親機に対して、自身が有するリソースを利用する利用権を発行する利用権発行ステップと

25 を含み、

前記端末が、前記親機から取得した前記利用権を提示した場合に、自身が有するリソースの利用を許可する

ことを特徴とする情報処理方法。

14. ユーザにより操作される端末に、自身が有するリソースを提供する情報処理装置に実行させるプログラムであって、

5 前記リソースの提供に対する対価としての電子バリューが、前記ユーザの個人情報
情報を記憶する親機から振り込まれたことの振込み通知を、電子バリューを管理
するバリュー装置から受信する振込み通知受信ステップと、

前記振込み通知に応じて、前記親機に対して、自身が有するリソースを利用す
る利用権を発行する利用権発行ステップと

を含み、

10 前記端末が、前記親機から取得した前記利用権を提示した場合に、自身が有す
るリソースの利用を許可する

ことを特徴とするプログラム。

15. ユーザにより操作される端末の前記ユーザの個人情報情報を記憶する情報処
理装置において、

15 前記端末からの要求に応じて、前記端末にリソースを提供する親機への、前記
リソースの提供に対する対価としての電子バリューの振込みを、電子バリューを
管理するバリュー装置に要求する電子バリュー振込み要求手段と、

前記電子バリューの振込みに応じて、前記親機が発行する、その親機が有する
リソースを利用する利用権を取得する利用権取得手段と、

20 前記利用権取得手段において取得された前記利用権を、前記端末に提供する利
用権提供手段と

を備えることを特徴とする情報処理装置。

16. 前記バリュー装置との間で、前記電子バリューを扱う正当な装置である
ことの認証を行う認証手段をさらに備える

25 ことを特徴とする請求の範囲第15項に記載の情報処理装置。

17. 前記端末との間で、前記ユーザが前記個人情報に対応する正当なユーザ
であることの認証を行う認証手段をさらに備える

ことを特徴とする請求の範囲第 15 項に記載の情報処理装置。

18. 前記リソースは、装置、情報、または情報に対するライセンスである

ことを特徴とする請求の範囲第 15 項に記載の情報処理装置。

19. ユーザにより操作される端末の前記ユーザの個人情報記憶する情報処理装置の情報処理方法において、

前記端末からの要求に応じて、前記端末にリソースを提供する親機への、前記リソースの提供に対する対価としての電子バリューの振込みを、電子バリューを管理するバリュー装置に要求する電子バリュー振込み要求ステップと、

10 前記電子バリューの振込みに応じて、前記親機が発行する、その親機が有するリソースを利用する利用権を取得する利用権取得ステップと、

前記利用権取得ステップの処理において取得された前記利用権を、前記端末に提供する利用権提供ステップと

を含むことを特徴とする情報処理方法。

20. ユーザにより操作される端末の前記ユーザの個人情報記憶する情報処理装置に実行させるプログラムにおいて、

前記端末からの要求に応じて、前記端末にリソースを提供する親機への、前記リソースの提供に対する対価としての電子バリューの振込みを、電子バリューを管理するバリュー装置に要求する電子バリュー振込み要求ステップと、

20 前記電子バリューの振込みに応じて、前記親機が発行する、その親機が有するリソースを利用する利用権を取得する利用権取得ステップと、

前記利用権取得ステップの処理において取得された前記利用権を、前記端末に提供する利用権提供ステップと

を含むことを特徴とするプログラム。

21. 電子バリューを管理する情報処理装置において、

25 ユーザにより操作される端末にリソースを提供する第 1 の親機に対する、そのリソースの提供に対する対価としての電子バリューの振込みを、前記ユーザの個人情報記憶する第 2 の親機からの要求に応じて行う電子バリュー振込み手段と、

前記第 2 の親機から前記第 1 の親機への前記電子バリューの振込みが行われたことを表す振込み通知を、前記第 1 の親機に送信する振込み通知送信手段とを備えることを特徴とする情報処理装置。

2 2. 前記第 1 または第 2 の親機との間で、前記電子バリューを扱う正当な装置であることの認証を行う認証手段を

さらに備えることを特徴とする請求の範囲第 2 1 に記載の情報処理装置。

2 3. 前記第 1 と第 2 の親機の電子バリューを記憶する記憶手段をさらに備え、前記電子バリュー振込み手段は、前記記憶手段に記憶された電子バリューを書き換えることにより、前記第 2 の親機から前記第 1 の親機に対して、前記電子バ

10 リューを振り込む

ことを特徴とする請求の範囲第 2 1 項に記載の情報処理装置。

2 4. 前記電子バリュー振込み手段は、前記第 2 の親機から電子バリューを取得し、その電子バリューを前記第 1 の親機に送信することにより、前記第 2 の親機から前記第 1 の親機に対して、前記電子バリューを振り込む

15 ことを特徴とする請求の範囲第 2 1 項に記載の情報処理装置。

2 5. 前記リソースは、装置、情報、または情報に対するライセンスであることを特徴とする請求の範囲第 2 1 項に記載の情報処理装置。

2 6. 前記電子バリューは、口座という形で管理され、

前記口座は、前記親機の証明書にある機器 ID、または、その機器 ID に対応
20 付けられた ID により管理される

ことを特徴とする請求の範囲第 2 1 項に記載の情報処理装置。

2 7. 電子バリューを管理する情報処理装置の情報処理方法において、

ユーザにより操作される端末にリソースを提供する第 1 の親機に対する、そのリソースの提供に対する対価としての電子バリューの振込みを、前記ユーザの個人情報
25 情報を記憶する第 2 の親機からの要求に応じて行う電子バリュー振込みステップと、

前記第 2 の親機から前記第 1 の親機への前記電子バリューの振込みが行われたことを表す振込み通知を、前記第 1 の親機に送信する振込み通知送信ステップとを含むことを特徴とする情報処理方法。

28. 電子バリューを管理する情報処理装置に実行させるプログラムであって、

- 5 ユーザにより操作される端末にリソースを提供する第 1 の親機に対する、そのリソースの提供に対する対価としての電子バリューの振込みを、前記ユーザの個人情報記憶する第 2 の親機からの要求に応じて行う電子バリュー振込みステップと、

- 10 前記第 2 の親機から前記第 1 の親機への前記電子バリューの振込みが行われたことを表す振込み通知を、前記第 1 の親機に送信する振込み通知送信ステップとを含むことを特徴とするプログラム。

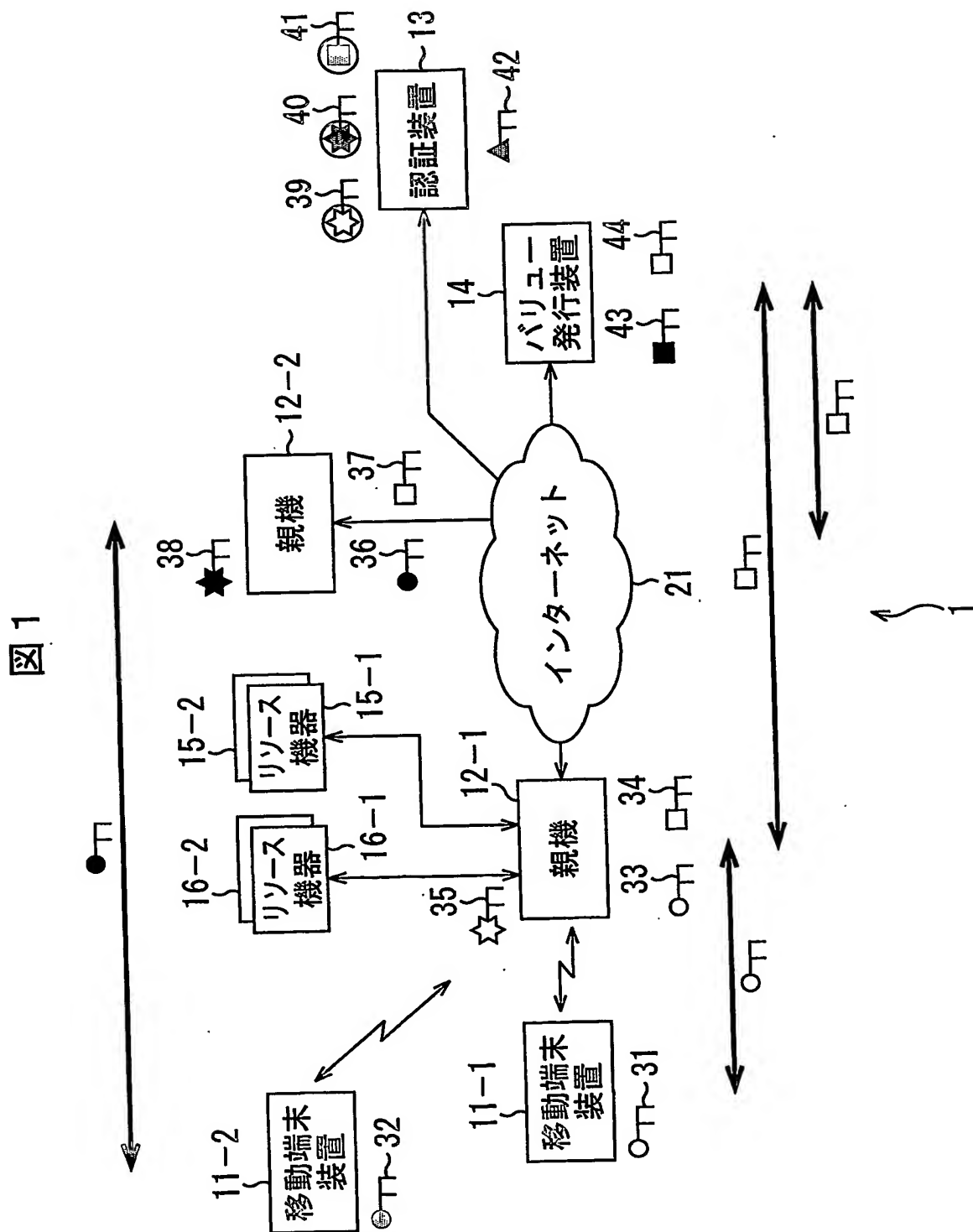
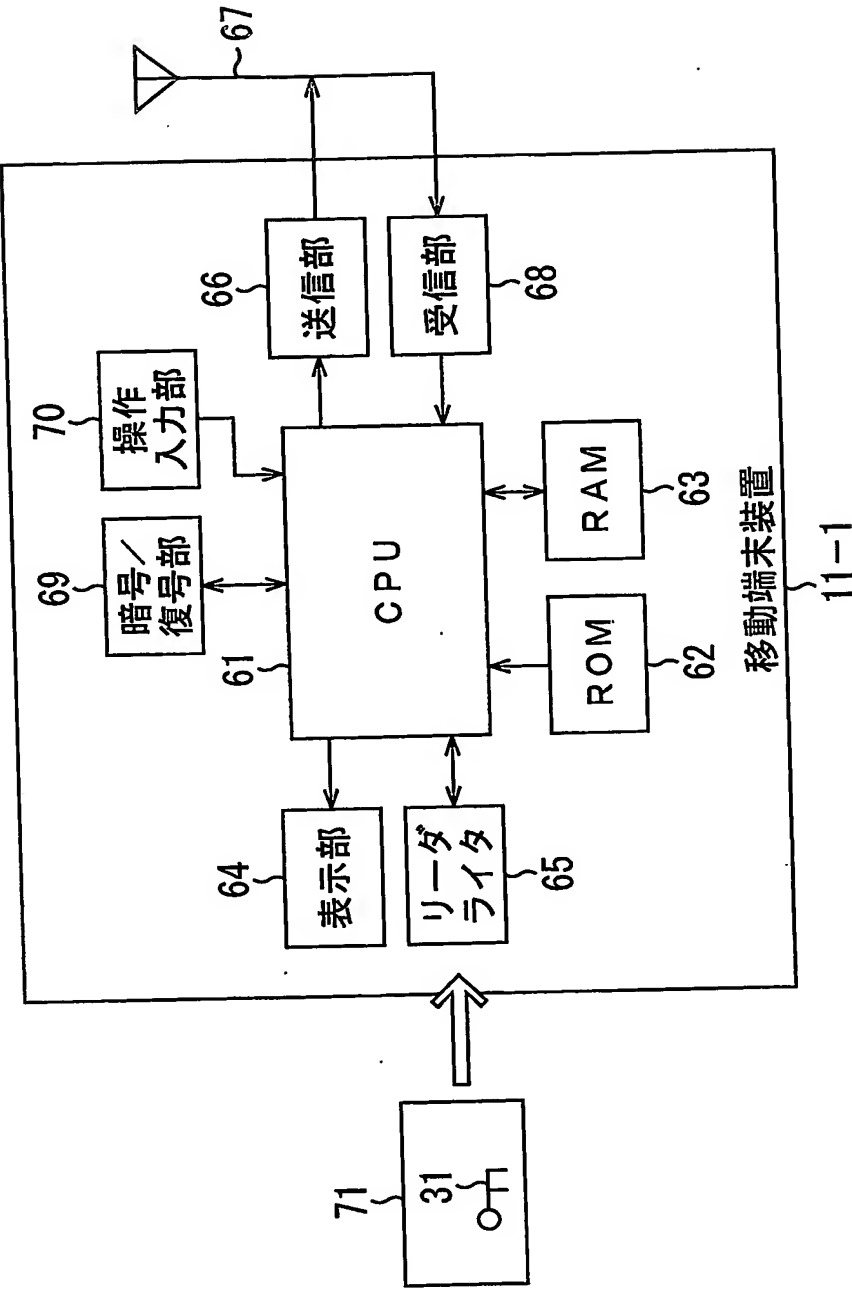
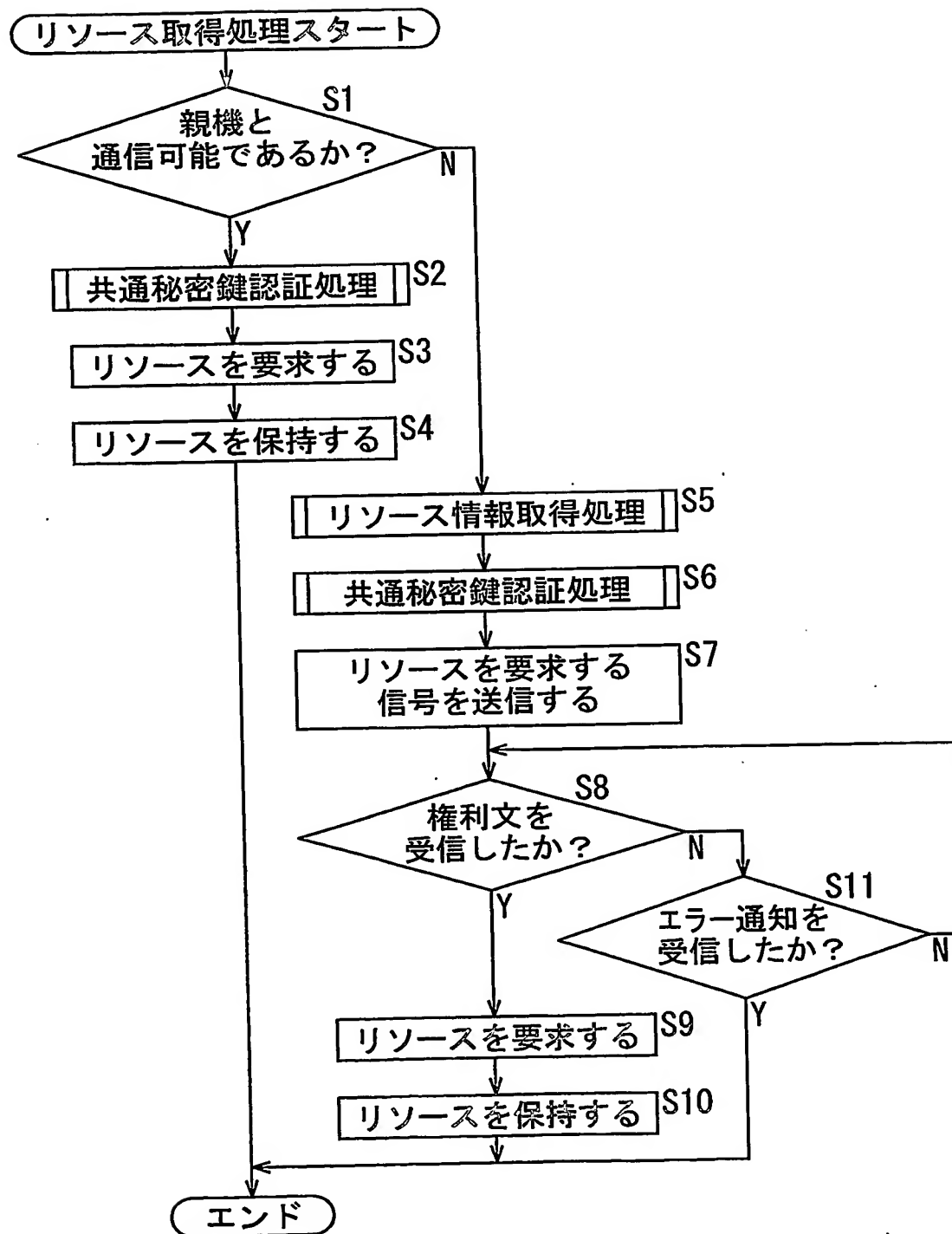


図2



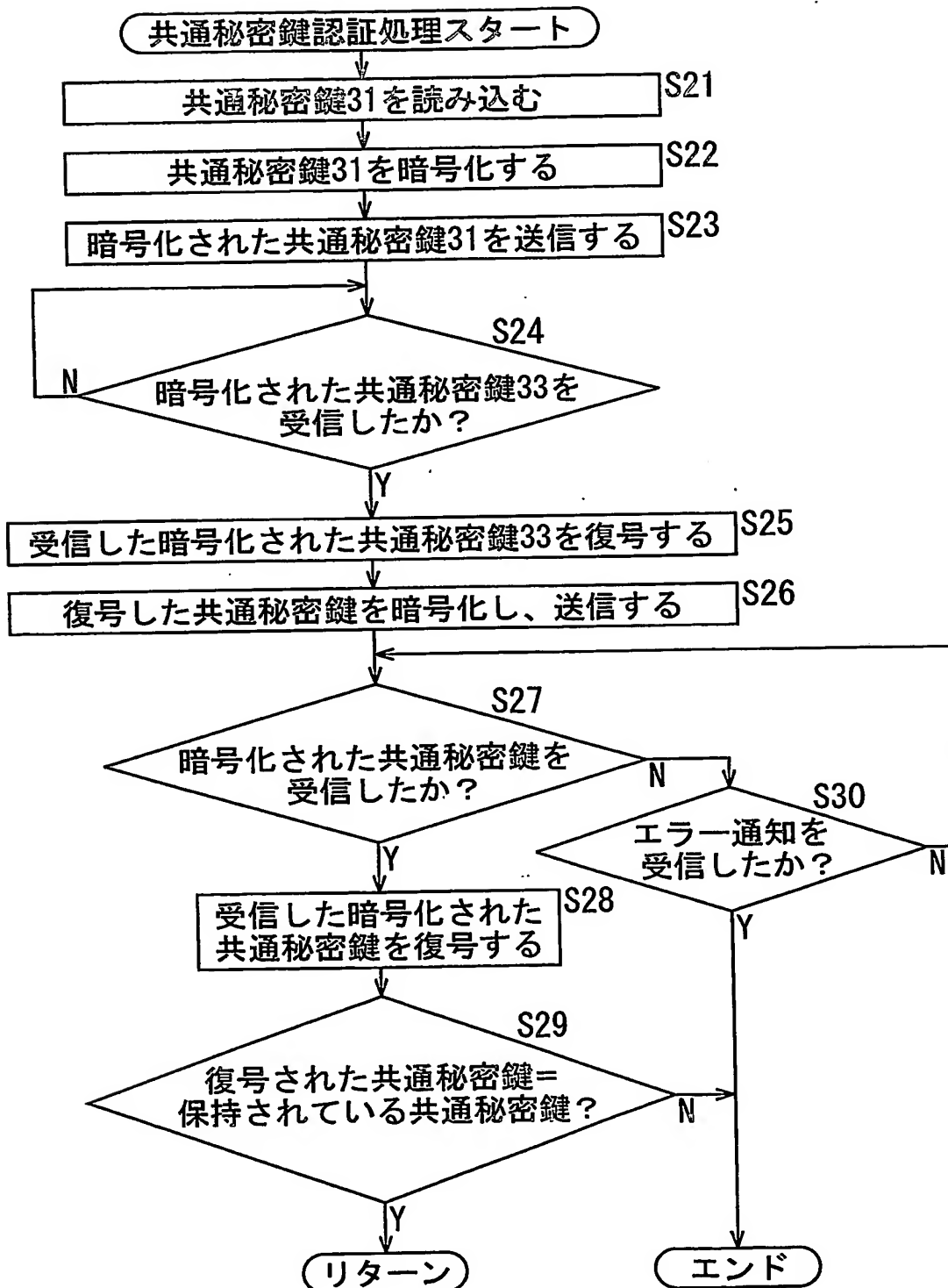
3/21

図 3



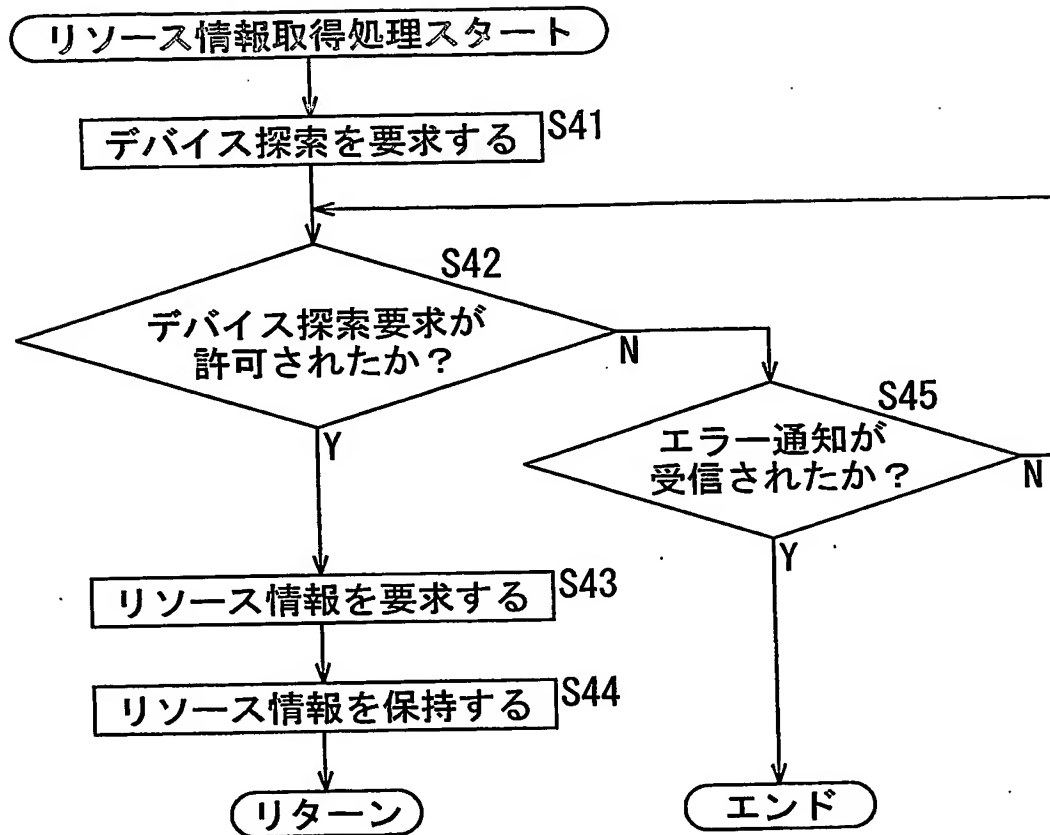
4/21

図 4



5/21

図 5



6/21

図6

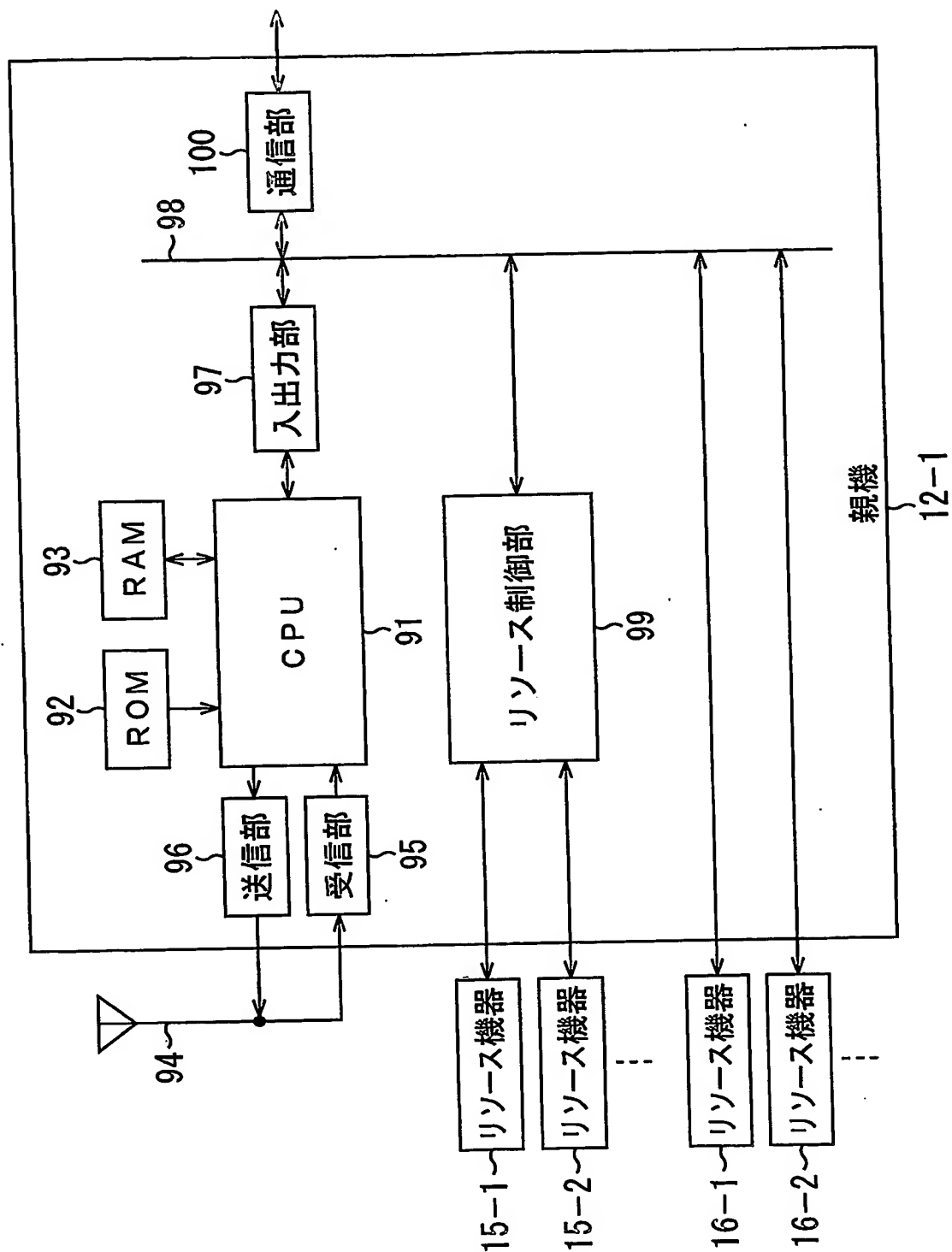
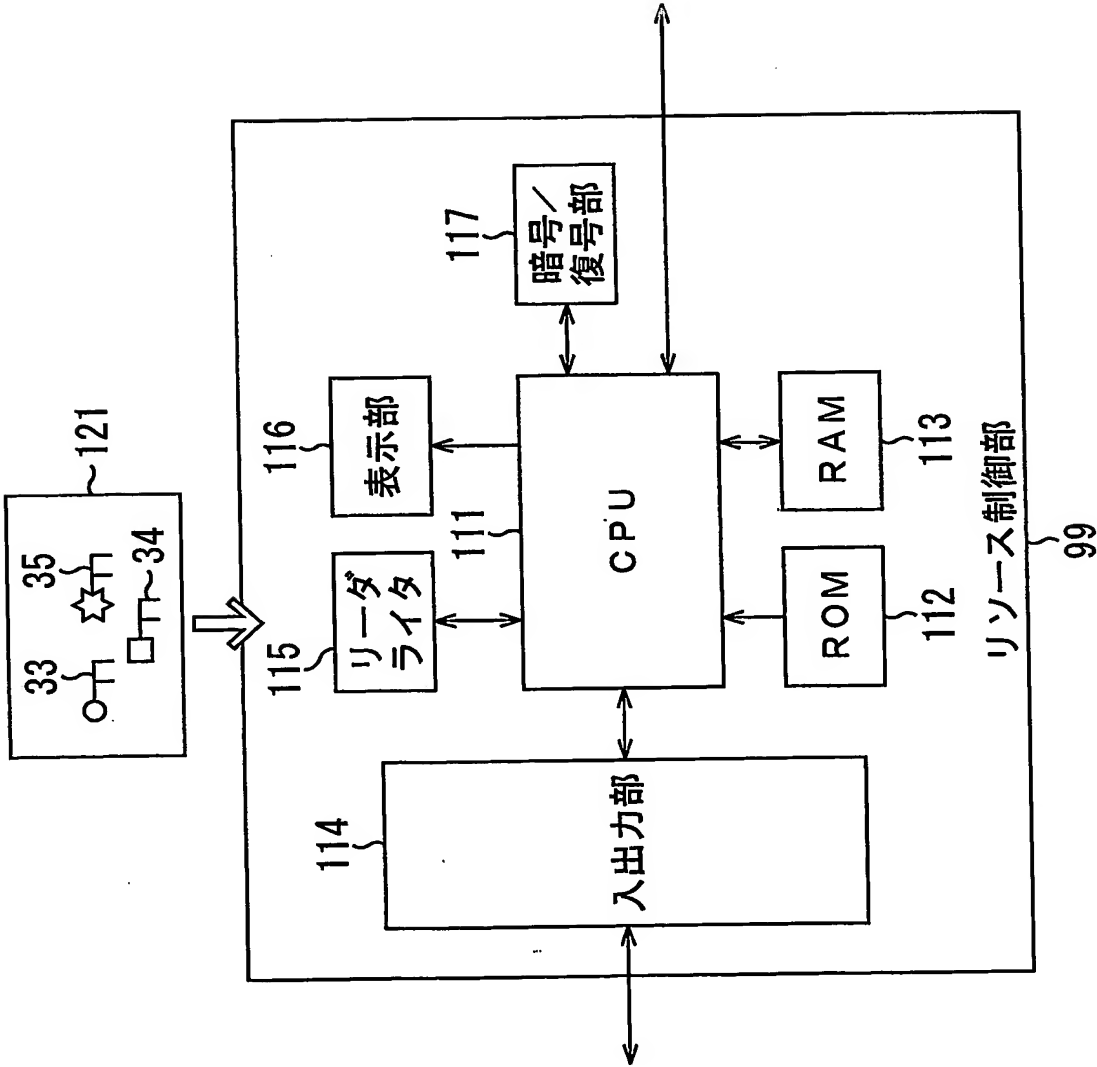
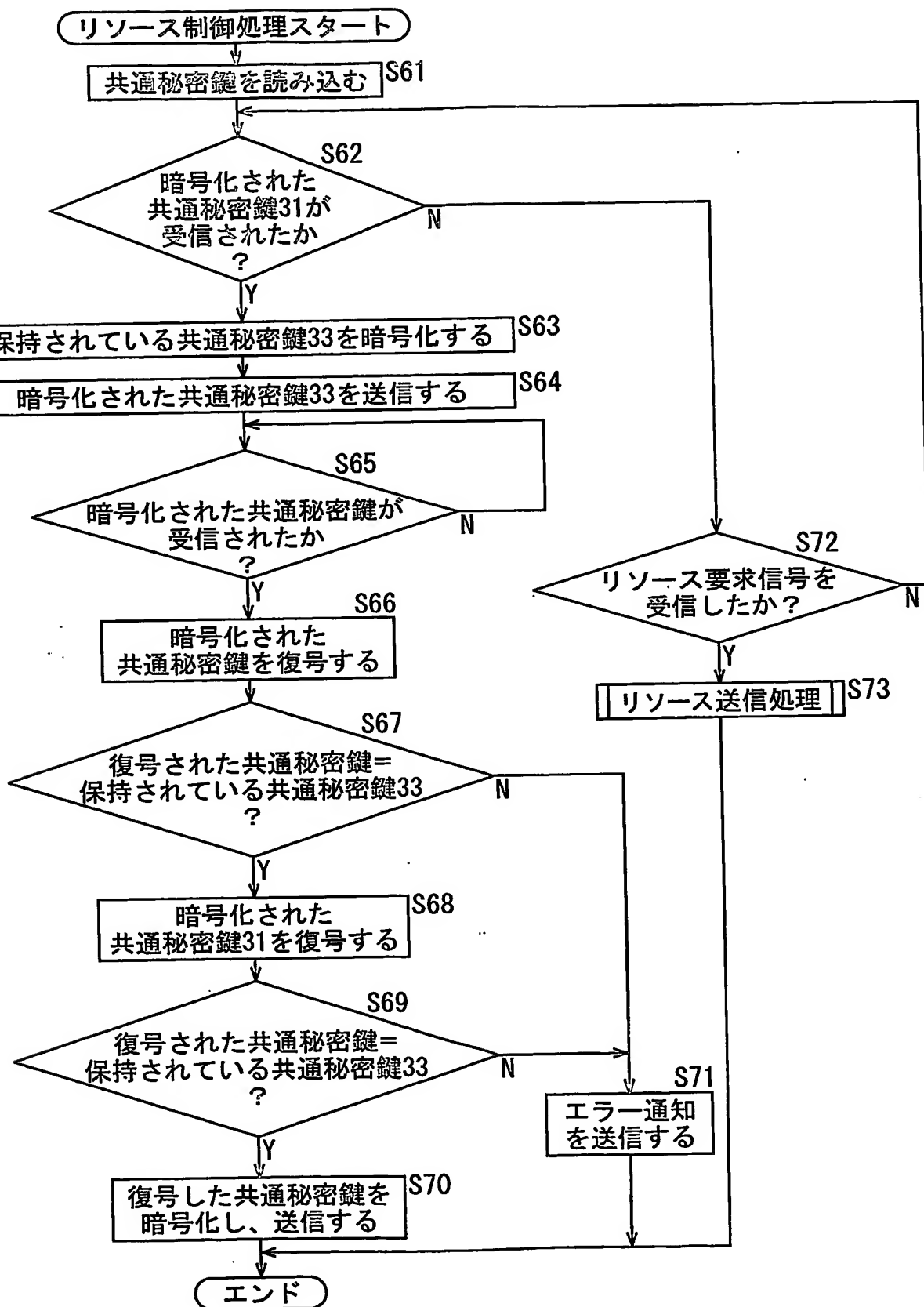


図 7



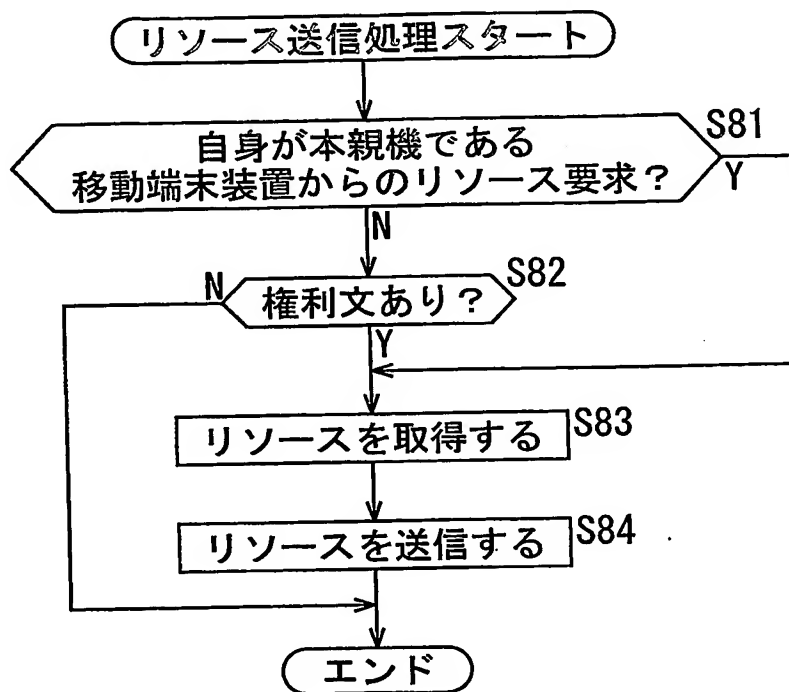
8/21

図 8



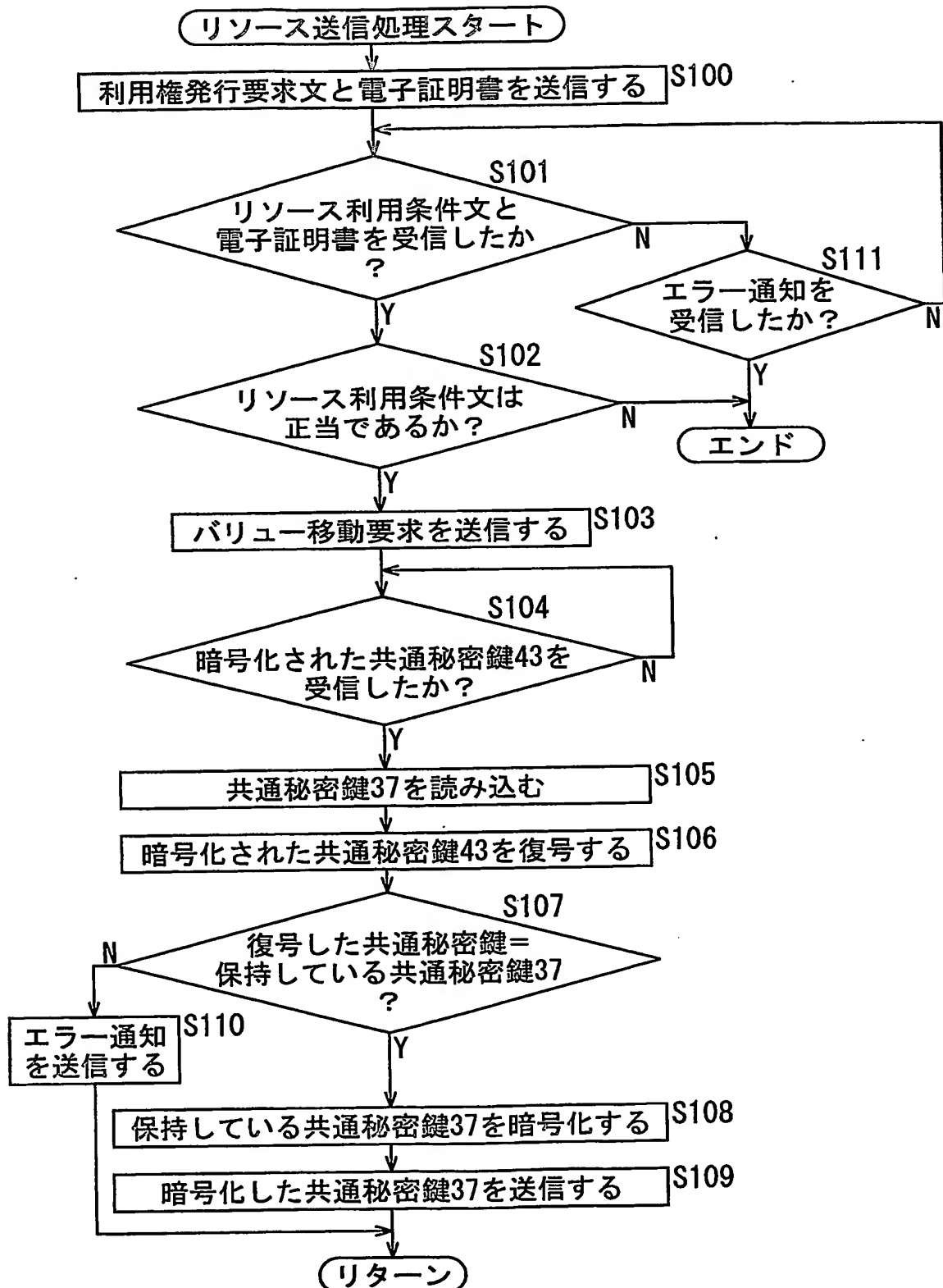
9/21

図 9



10/21

図10



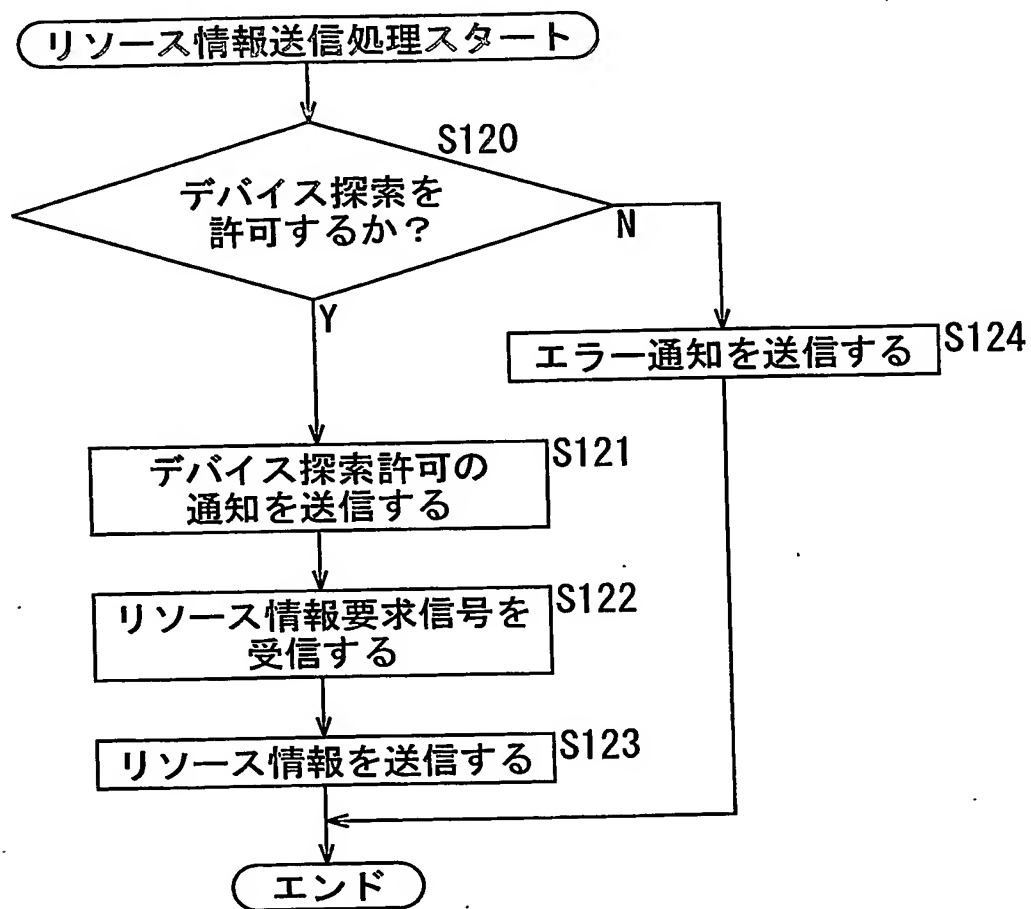
11/21

図11

電子証明書
証明書のバージョン番号
証明書の通し番号
署名に用いたアルゴリズムとパラメータ
認証局の名前
証明書の有効期限
装置のID
装置の公開鍵

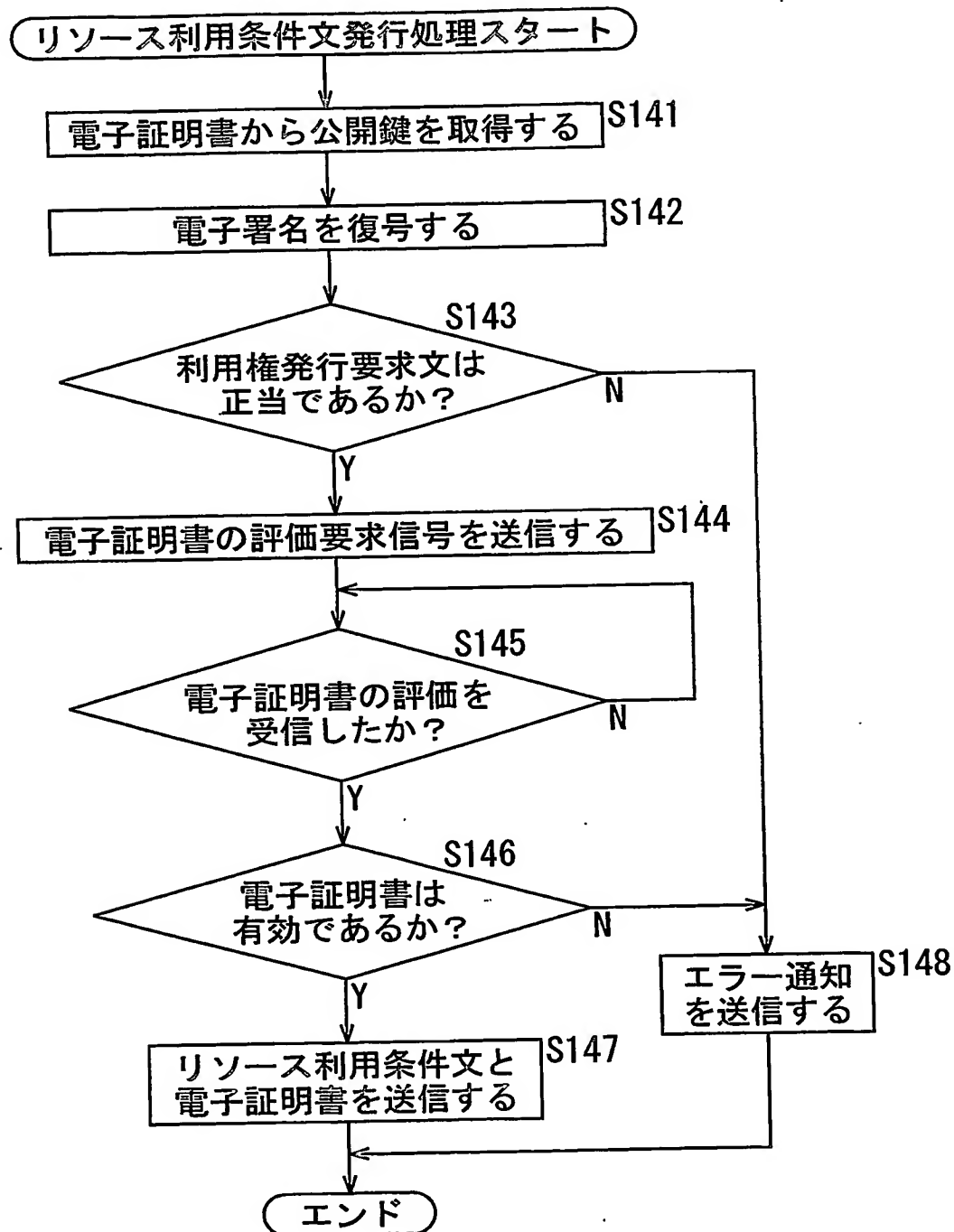
12/21

図12



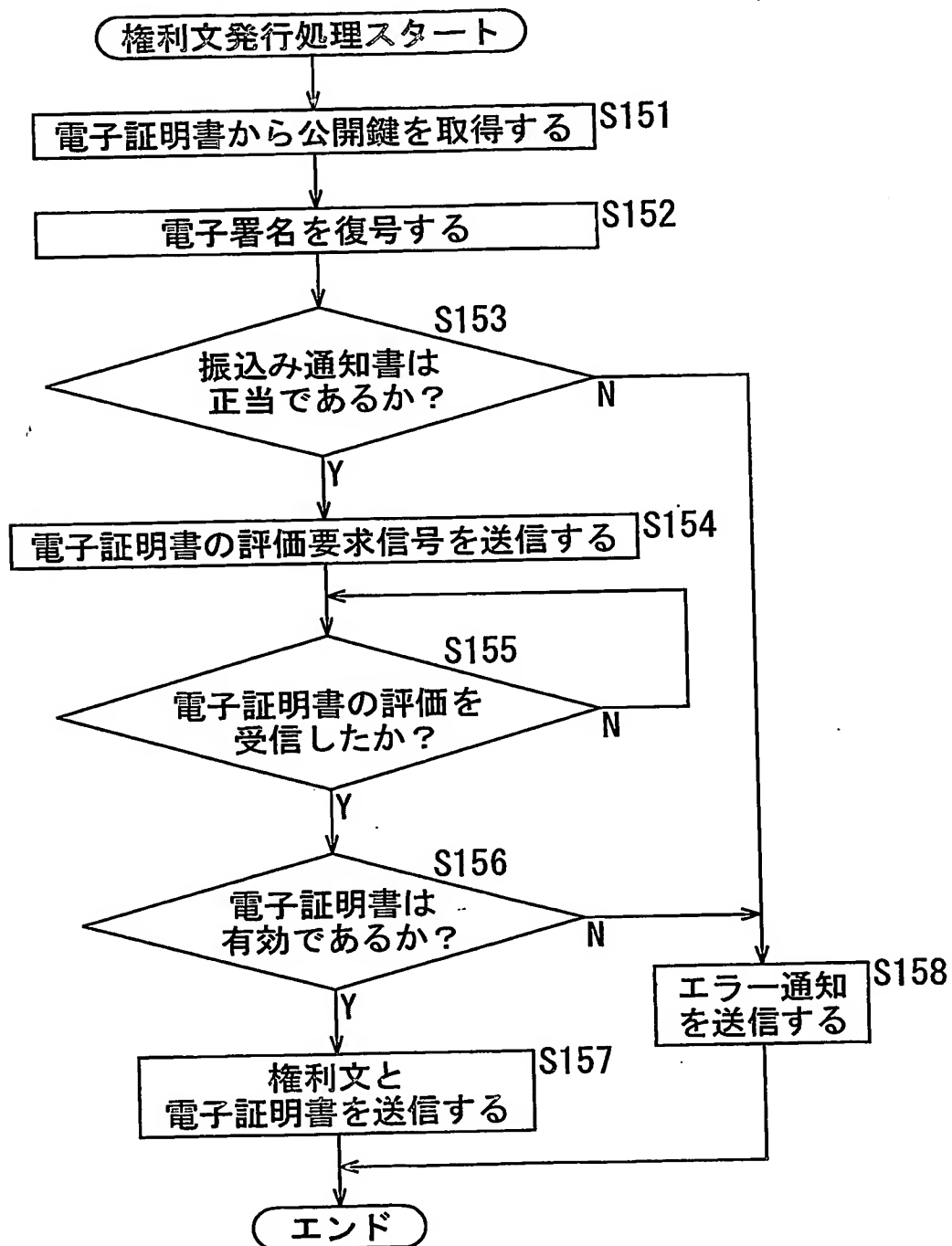
13/21

図13



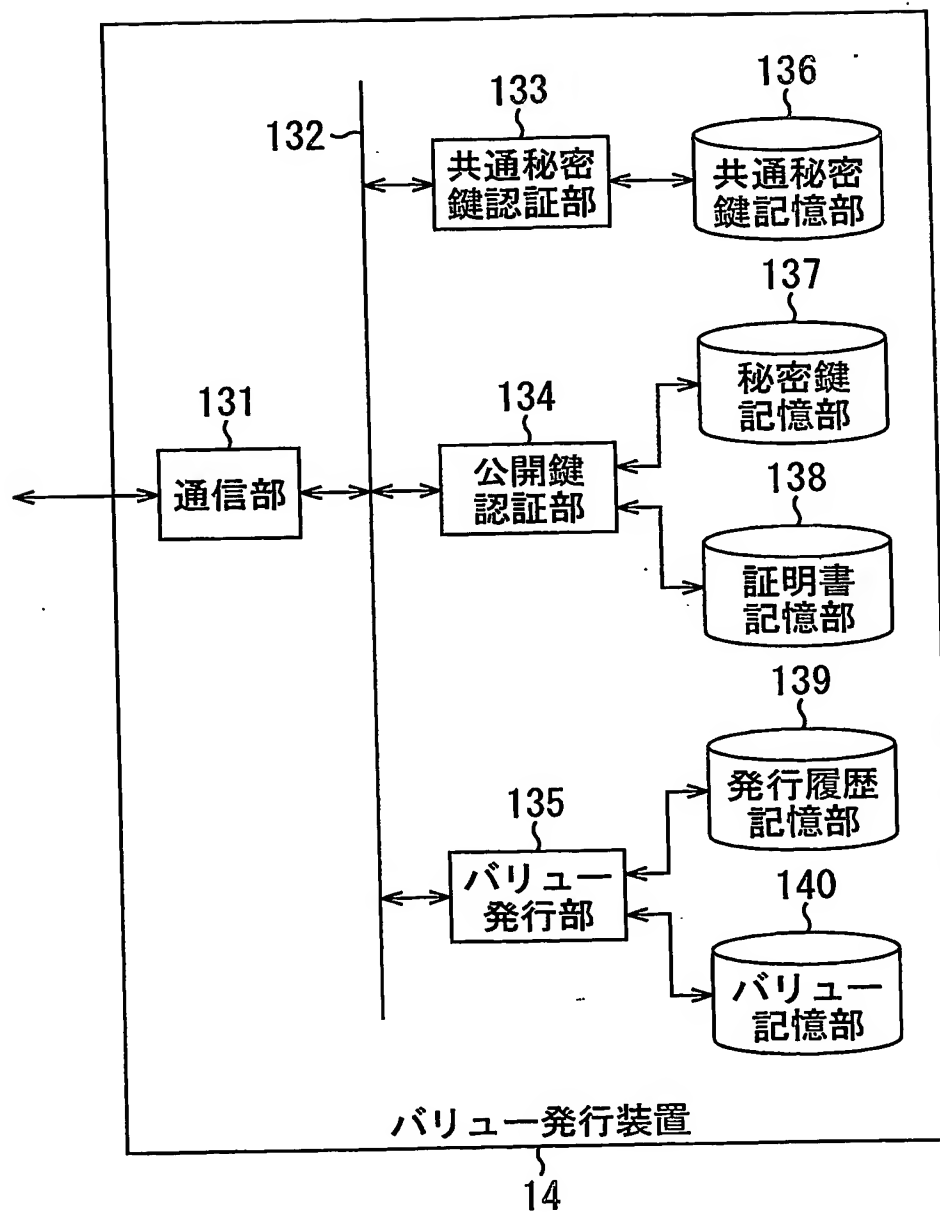
14/21

図14



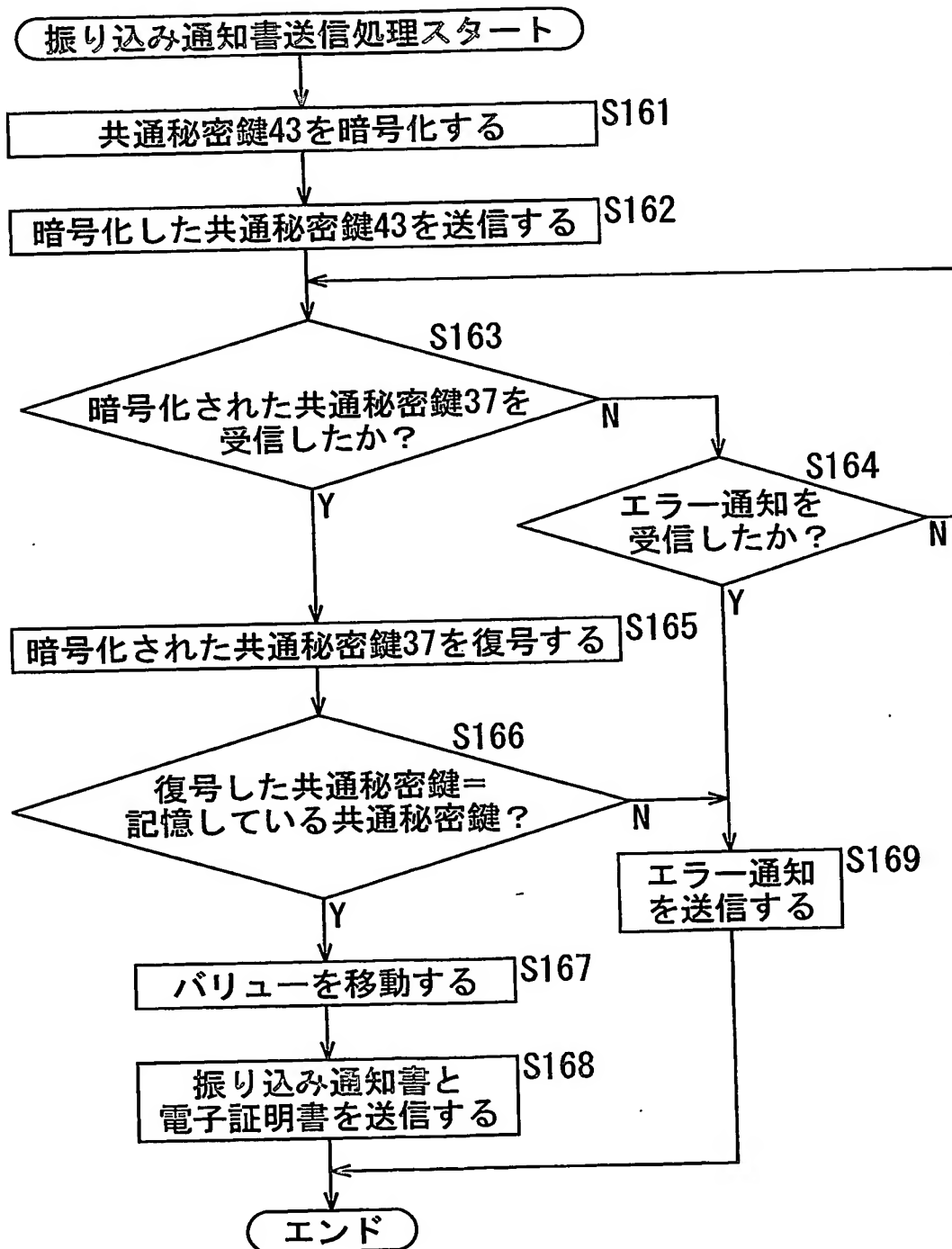
15/21

図15



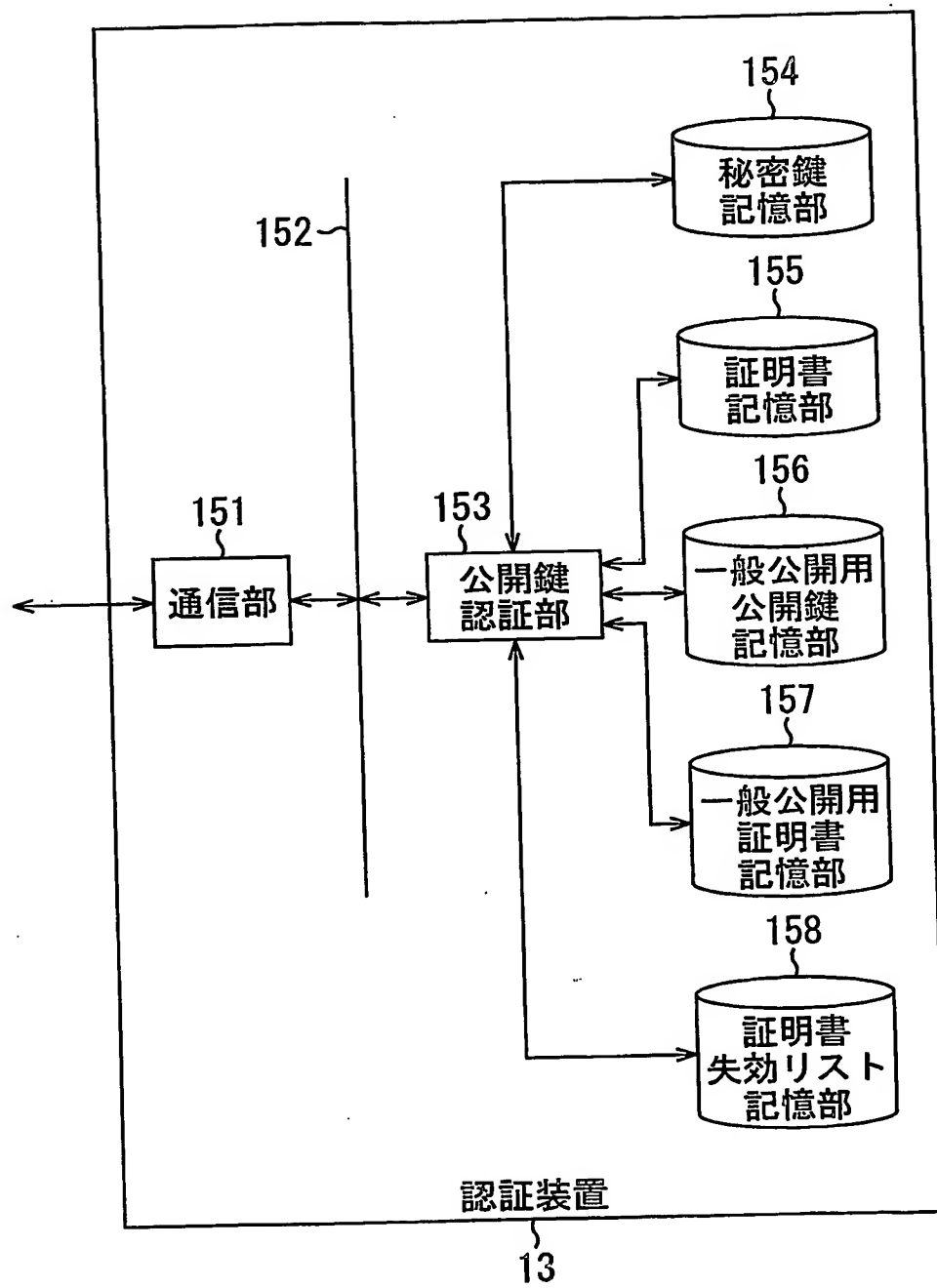
16/21

図16



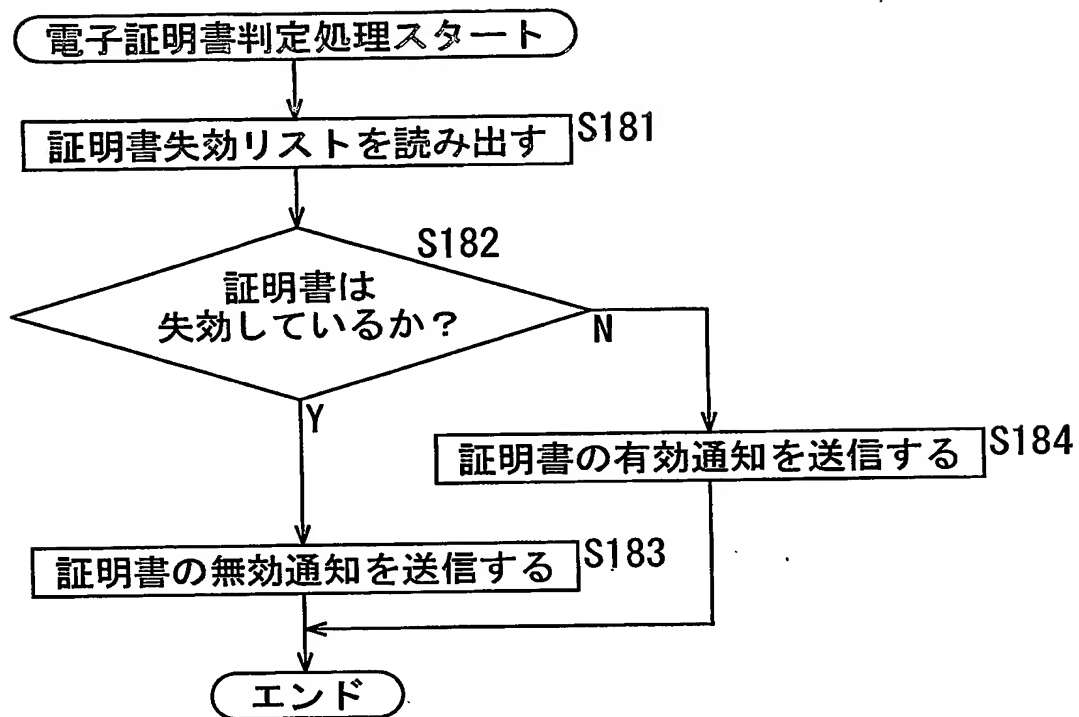
17/21

図17



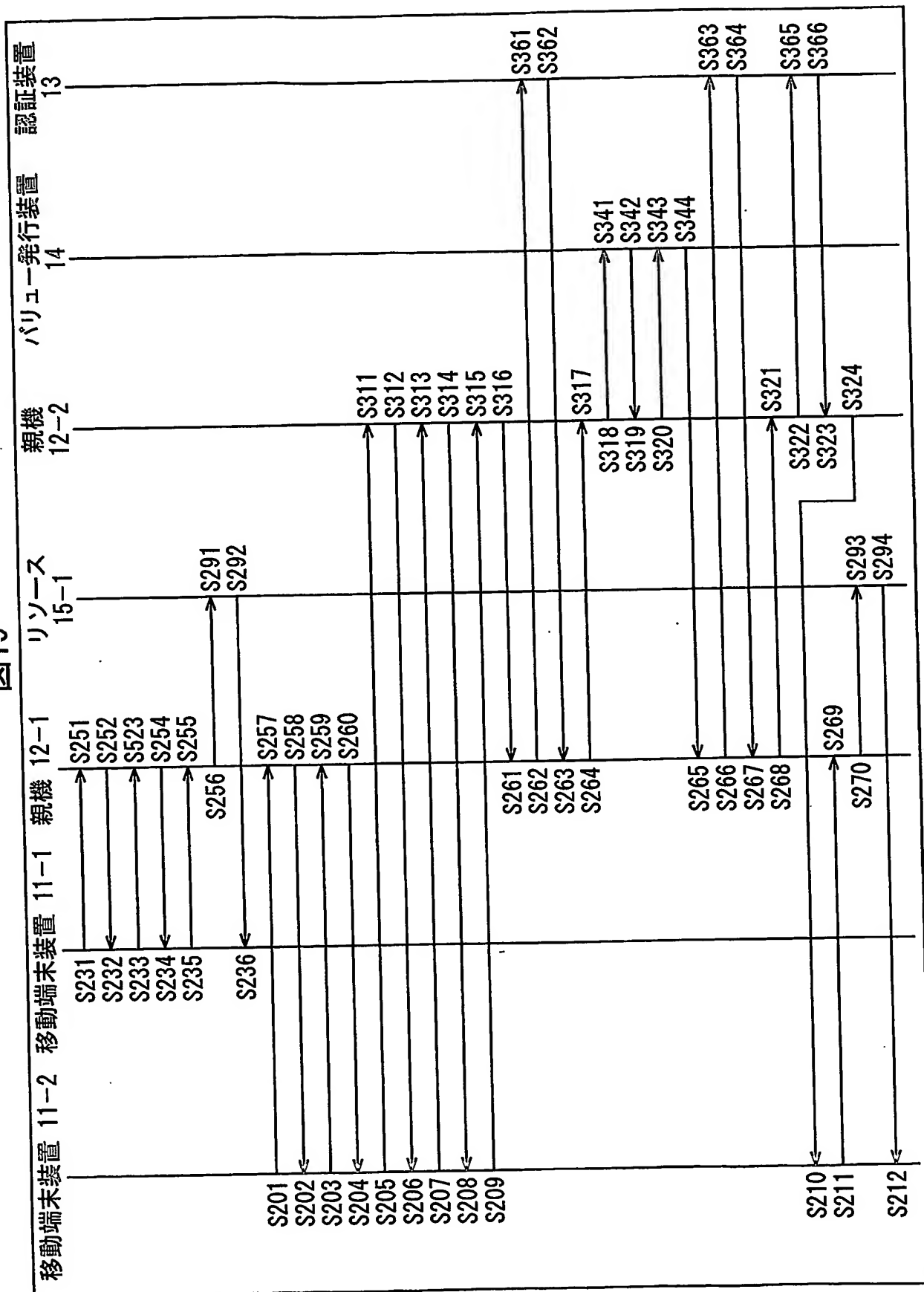
18/21

図18



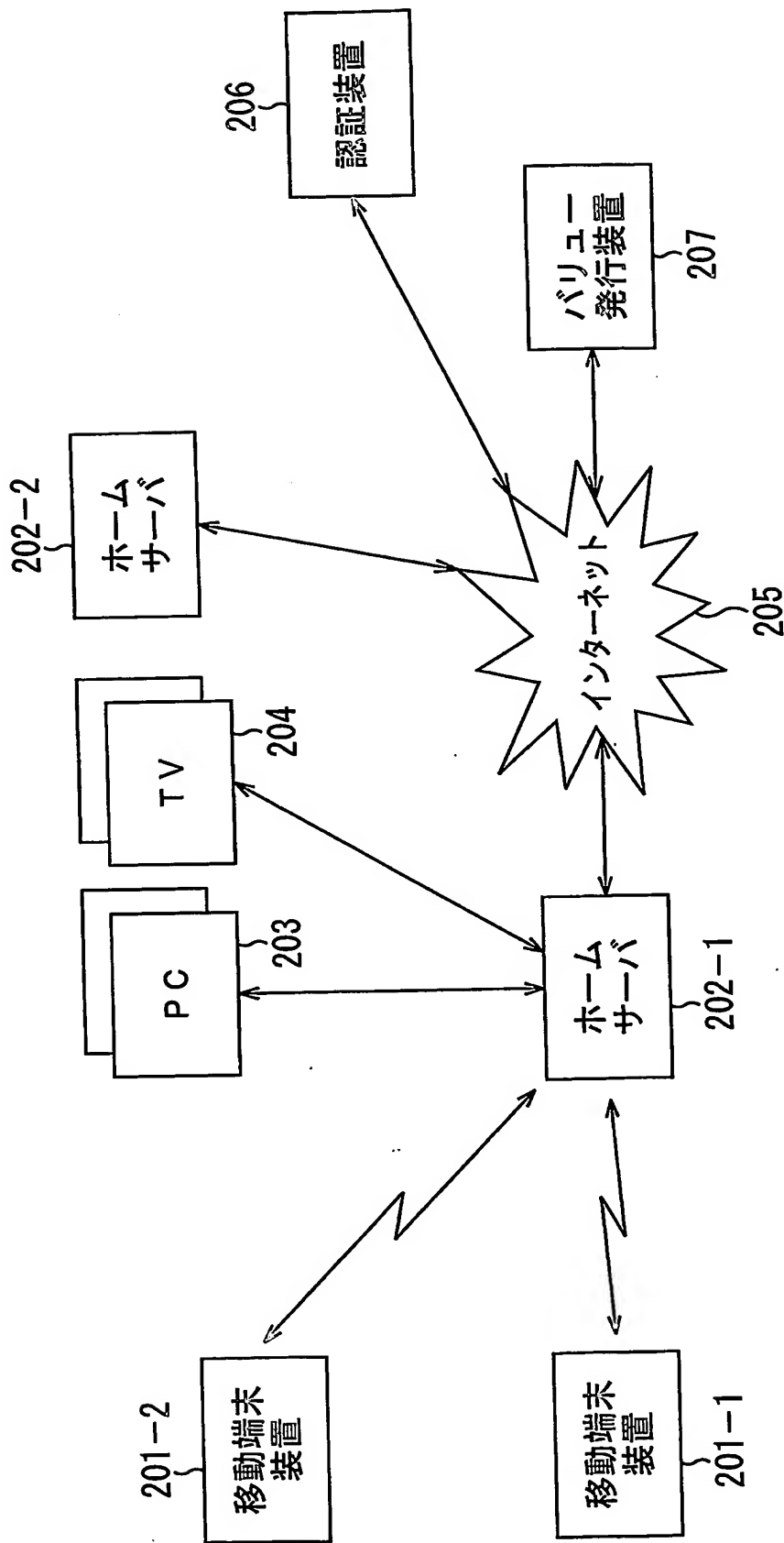
19/21

図19



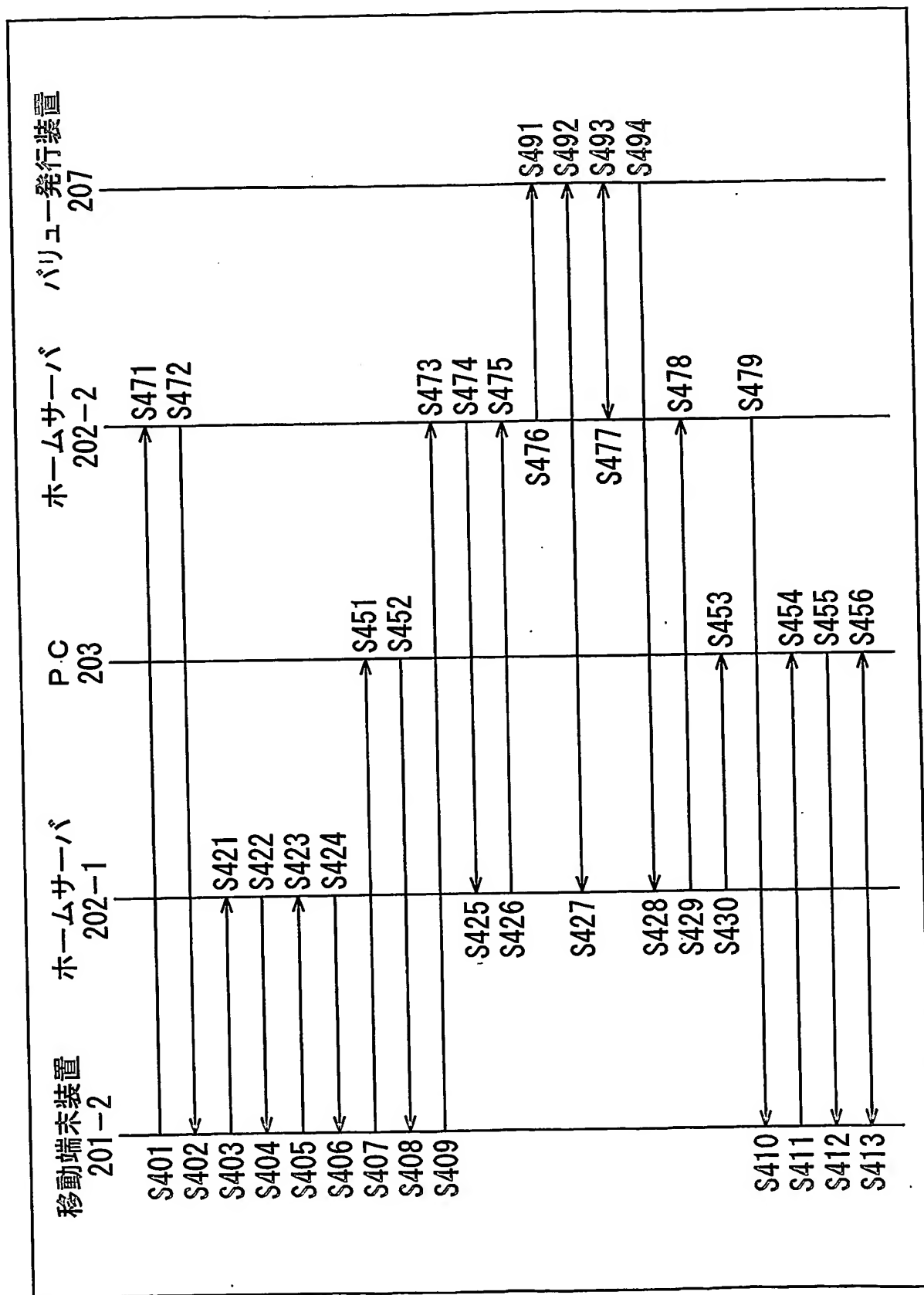
20/21

図20



21/21

図21



INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2004/004338

A. CLASSIFICATION OF SUBJECT MATTER

Int.Cl⁷ G06F17/60

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

Int.Cl⁷ G06F17/60, G06F15/00

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Jitsuyo Shinan Koho	1922-1996	Toroku Jitsuyo Shinan Koho	1994-2004
Kokai Jitsuyo Shinan Koho	1971-2004	Jitsuyo Shinan Toroku Koho	1996-2004

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
JICST FILE (JOIS)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	JP 2002-323986 A (Hitachi, Ltd.), 08 November, 2002 (08.11.02), & US 2002/161891 A1	1-28
A	JP 2002-140295 A (Nippon Telegraph And Telephone Corp.), 17 May, 2002 (17.05.02), (Family: none)	1-28
A	JP 2002-73566 A (Sony Corp.), 12 March, 2002 (12.03.02), & US 2002/26427 A1	1-28
A	Tatsuo ITABASHI et al., "Hisesshoku IC card to Keitai Joho Tanmatsu o Riyo shita E-Commerce system no Kaihatsu", Proceedings of Sony Research Forum, 2001, 2002, Vol.11, pages 125 to 130	1-28

☐ Further documents are listed in the continuation of Box C.

☐ See patent family annex.

* Special categories of cited documents:
 "A" document defining the general state of the art which is not considered to be of particular relevance
 "E" earlier application or patent but published on or after the international filing date
 "L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
 "O" document referring to an oral disclosure, use, exhibition or other means
 "P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
 "X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
 "Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
 "&" document member of the same patent family

Date of the actual completion of the international search
19 April, 2004 (19.04.04)

Date of mailing of the international search report
11 May, 2004 (11.05.04)

Name and mailing address of the ISA/
Japanese Patent Office

Authorized officer

Facsimile No.

Telephone No.

A. 発明の属する分野の分類 (国際特許分類 (IPC))

Int Cl⁷ G06F17/60

B. 調査を行った分野

調査を行った最小限資料 (国際特許分類 (IPC))

Int Cl⁷ G06F17/60, G06F15/00

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報	1922-1996年
日本国公開実用新案公報	1971-2004年
日本国登録実用新案公報	1994-2004年
日本国実用新案登録公報	1996-2004年

国際調査で使用した電子データベース (データベースの名称、調査に使用した用語)

JICSTファイル (JOIS)

C. 関連すると認められる文献

引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
A	JP 2002-323986 A (株式会社日立製作所) 2002. 11. 08 & US 2002/161891 A1	1-28
A	JP 2002-140295 A (日本電信電話株式会社) 2002. 05. 17 (ファミリーなし)	1-28
A	JP 2002-73566 A (ソニー株式会社) 2002. 03. 12 & US 2002/26427 A1	1-28

☒ C欄の続きにも文献が列挙されている。☐ パテントファミリーに関する別紙を参照。

* 引用文献のカテゴリー

「A」 特に関連のある文献ではなく、一般的技術水準を示すもの
「E」 国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
「L」 優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献 (理由を付す)
「O」 口頭による開示、使用、展示等に言及する文献
「P」 国際出願日前で、かつ優先権の主張の基礎となる出願

の日の後に公表された文献

「T」 国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
「X」 特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
「Y」 特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
「&」 同一パテントファミリー文献

国際調査を完了した日

19. 04. 2004

国際調査報告の発送日 11. 5. 2004

国際調査機関の名称及びあて先

日本国特許庁 (ISA/JP)
郵便番号 100-8915

東京都千代田区霞が関三丁目4番3号

特許庁審査官 (権限のある職員)

金子 幸一

5 L

8724

電話番号 03-3581-1101 内線 3560

C (続き) . 関連すると認められる文献		
引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
A	板橋達夫他, 非接触 I C カードと携帯情報端末を利用した e コマースシステムの開発, Proceedings of Sony Research Forum 2001, 2002, 第 11 巻, p. 125-130	1-28

**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☒ **BLACK BORDERS**
- ☐ **IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**
- ☐ **FADED TEXT OR DRAWING**
- ☐ **BLURRED OR ILLEGIBLE TEXT OR DRAWING**
- ☐ **SKEWED/SLANTED IMAGES**
- ☐ **COLOR OR BLACK AND WHITE PHOTOGRAPHS**
- ☐ **GRAY SCALE DOCUMENTS**
- ☐ **LINES OR MARKS ON ORIGINAL DOCUMENT**
- ☐ **REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**
- ☐ **OTHER:** _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.